Australian Government
Productivity Commission

Public Safety Mobile Broadband

Productivity Commission
Draft Report

September 2015

This draft report has been prepared for further public consultation and input.
The Commission will finalise its report after these processes have taken place.

An appropriate reference for this publication is:

Productivity Commission 2015, *Public Safety Mobile Broadband,* Draft Report, Canberra.

Publications enquiries

Media and Publications, phone: (03) 9653 2244 or email: maps@pc.gov.au

The Productivity Commission

The Productivity Commission is the Australian Government's independent research and advisory body on a range of economic, social and environmental issues affecting the welfare of Australians. Its role, expressed most simply, is to help governments make better policies, in the long term interest of the Australian community.

The Commission's independence is underpinned by an Act of Parliament. Its processes and outputs are open to public scrutiny and are driven by concern for the wellbeing of the community as a whole.

Further information on the Productivity Commission can be obtained from the Commission's website (www.pc.gov.au).

Opportunity for further comment

You are invited to examine this draft report and comment on it by written submission to the Productivity Commission, preferably in electronic format, by **Wednesday 28 October 2015**. Further information on how to provide a submission is included on the study website: http://www.pc.gov.au/inquiries/current/public-safety-mobile-broadband/make-submission.

The final report will be prepared after further submissions have been received.

Commissioners

For the purposes of this study the Commissioner is:

Jonathan Coppel Presiding Commissioner

Terms of reference

**Public Safety Mobile Broadband
Terms of Reference**

I, Joseph Benedict Hockey, Treasurer, pursuant to Parts 2 and 4 of the *Productivity Commission Act 1998*, hereby request that the Productivity Commission (the Commission) undertake a study into the best way to secure a mobile broadband capability to meet the long term needs of Australia's public safety agencies (PSAs): the police, fire, ambulance and emergency services.

Background

A robust and effective mobile broadband capability is a critical enabler for Australia's PSAs.

Since June 2011, the Commonwealth has worked with jurisdictions and PSAs — through the Council of Australian Governments (COAG) Public Safety Mobile Broadband (PSMB) Steering Committee — to consider how best to deliver a strong PSMB capability. On 19 April 2013, COAG transferred responsibility for PSMB from the Steering Committee to COAG Senior Officials and, in doing so, noted the need for PSAs to have adequate capabilities to respond efficiently and effectively when disasters occur.

Delivering a PSMB capability is complex and involves using scarce and valuable resources, such as radiocommunications spectrum, to further the public interest. To inform this work and ensure the best path forward, the Commonwealth considers it appropriate to undertake a rigorous analysis of the most efficient, effective and economical means of developing Australia's PSMB capability.

Scope of the study

The Commission is to undertake a 'first principles' analysis of the most efficient, effective and economical way of delivering this capability by 2020, to coincide with the nationally agreed framework to improve government radio communications, including interoperability.[1] Particular regard should be given to:

[1] This is outlined in the COAG-endorsed National Framework to Improve Government Radiocommunications Interoperability 2010–2020.

1. The most cost-effective combination of private and public inputs, services and expertise to deliver the capability. This should include an assessment of the relative costs, benefits and risks of:
   a. deploying a dedicated PSMB network
   b. an approach that is fully reliant on commercial networks, and/or
   c. a combination of the two.

2. The ability for the capability to:
   a. be nationally interoperable, within and across agencies and jurisdictions
   b. operate in both metropolitan and regional Australia
   c. integrate voice communications that are traditionally carried on narrowband networks
   d. maintain integrity and security of communications
   e. ensure accessibility, priority and sufficient capacity for PSAs, particularly during periods of peak demand and during a localised incident
   f. be resilient and maintain continuity of service including under adverse operating circumstances
   g. consider the sustainability of arrangements in the context of rapidly changing technology and increased demand, including convergence of voice and data services
   h. be cost-effective, in terms of both capital and operating cost
   i. be nationally available by or before 2020, and
   j. be compatible with a variety of end-user devices.

3. Relevant domestic and international reports and experiences (e.g. work underway through the Asia Pacific Telecommunity Wireless Group (AWG), International Telecommunication Union (ITU), 3rd Generation Partnership Project (3GPP) and implementation of similar capability in other countries) that may be applicable to Australia.

In conducting the analysis, the Commission is to have regard to the Australian Communications and Media Authority's (ACMA) role as the independent national regulator and technical expert on communications matters, with final decision-making responsibility for allocation of and conditions of access to spectrum. The Commission should also, where practicable, have regard to the Government's broader review of the spectrum policy and management framework.

Based on information provided by PSAs about their operational requirements, the ACMA has previously conducted an engineering analysis into the spectrum requirements for a PSMB capability. This analysis was carried out within parameters established by the Public Safety Mobile Broadband Steering Committee (PSMBSC) and the Terms of Reference for that committee. However, spectrum alone will not achieve a PSMB capability as infrastructure and supporting networks with compatible end-user equipment are required. The Commission's analysis is concerned with an overall consideration of the most efficient, effective and economical way of delivering this capability, including a re-evaluation of user needs and project requirements given the passage of time.

Process

The Commission is to consult broadly, including with industry and non-government stakeholders, state and territory governments, and PSAs and relevant Commonwealth agencies.

The Commission will produce a draft and a final Report, both of which will be published. The final Report is to be provided to the Government within nine months of the receipt of these Terms of Reference.

J.B. HOCKEY

Treasurer

[Received 25 March 2015]

Contents

Opportunity for further comment iii

Terms of reference iv

Abbreviations x

Glossary xiii

Overview 1

Draft recommendations, findings and information requests 31

1 Introduction 39

1.1 Background to the study 39

1.2 What has the Commission been asked to do? 40

1.3 Domestic and international experiences 40

1.4 Stakeholder perspectives on PSMB 44

1.5 The Commission's approach 46

1.6 Conduct of the study 47

1.7 Structure of the draft report 48

2 Public safety agency communications 49

2.1 Who are the public safety agencies? 50

2.2 PSA demand for communication services 51

2.3 How are PSAs communicating? 54

2.4 Operational and functional requirements of PSAs' communication services 57

2.5 Network infrastructure used to meet PSA communication needs 60

2.6 Institutions, governance and regulatory arrangements 74

2.7 Limitations of current PSA communication capabilities 78

3 Framework for analysis **81**
3.1 Mobile broadband can enhance public safety 82
3.2 The Commission’s first principles approach 88
4 What is a public safety mobile broadband capability? **97**
4.1 Key dimensions of a mobile broadband capability 98
4.2 How are PSAs different to other mobile broadband customers? 106
4.3 What do PSAs want from a PSMB capability? 111
4.4 PSMB scenarios for analytical purposes 122
5 How can a PSMB capability be delivered? **127**
5.1 Delivery approaches for PSMB 128
5.2 Understanding mobile networks 130
5.3 Coverage and capacity requirements 135
5.4 Delivering a preferential service capability 144
5.5 Network reliability 148
5.6 Interoperability and security 153
5.7 Timing and sustainability 159
5.8 Summing up 162
6 Evaluating PSMB options **165**
6.1 Options for evaluation 166
6.2 Evaluation of costs 172
6.3 Evaluation of risks 183
6.4 Differences in benefits between options 192
7 Implementing a PSMB capability **195**
7.1 Institutional and governance arrangements 196
7.2 National coordination and standards 206
7.3 Spectrum allocation 210
7.4 The role of regulation 216
7.5 Public procurement 221
7.6 A phased approach to implementation 234

A Public consultation **239**

B Domestic and international developments in PSMB **245**

B.1 Previous Australian reviews and policy background 245

B.2 International spectrum harmonisation and technical standards 248

B.3 Approach to PSMB in other countries 252

C Quantitative methodology and results **269**

C.1 About this appendix 269

C.2 Overview of the quantitative framework 270

C.3 Geotyping 272

C.4 RAN dimensioning 277

C.5 Network costing 283

C.6 Calibration and inputs 297

C.7 Results 311

C.8 Sensitivity testing 314

C.9 Excluded costs 363

References **367**

Abbreviations

2G	Second generation
3G	Third generation
3GPP	3rd Generation Partnership Project
4G	Fourth generation
5G	Fifth generation
ACCC	Australian Competition and Consumer Commission
ACMA	Australian Communications and Media Authority
APT	Asia-Pacific Telecommunity
BAU	Business as usual
bps	Bits per second
BSS	Business Support System
CAD	Computer Aided Dispatch
CBA	Cost–benefit analysis
CBD	Central business district
COAG	Council of Australian Governments
COW	Cell on wheels
GB	Gigabyte
GHz	Gigahertz
GPS	Global Positioning System
GRN	Government Radio Network
GSM	Global System for Mobile Communications
GWN	Government Wireless Network
HF	High frequency
HSDPA	High-Speed Downlink Packet Access
IC	Industry Commission
IP	Internet protocol
IT	Information technology

ITU	International Telecommunication Union
ITU-R	International Telecommunication Union radiocommunications sector
kbps	kilobits per second
LMR	Land mobile radio
LTE	Long Term Evolution
MAPL	Maximum allowable propagation loss
MB	Megabyte
Mbps	Megabits per second
MDN	Mobile Data Network
MHz	Megahertz
MIMO	Multiple Input Multiple Output
NBN	National Broadband Network
NCCGR	National Coordination Committee for Government Radiocommunications
NPV	Net present value
OSS	Operations Support System
P25	Project 25 digital radio
PC	Productivity Commission
PLMN	Public Land Mobile Network
PPDR	Public protection and disaster relief
PSA	Public safety agency
PSMB	Public safety mobile broadband
PSMBSC	Public Safety Mobile Broadband Steering Committee
PTT	Push to talk
QoS	Quality of service
RAN	Radio access network
SA1	Statistical Area Level 1
SA2	Statistical Area Level 2
SES	State Emergency Service
SIM	Subscriber Identity Module
SMS	Short Message Service
TETRA	Terrestrial Trunked Radio

UHF	Ultra High Frequency
USIM	Universal Subscriber Identity Module
VHF	Very High Frequency
WCDMA	Wideband Code Division Multiple Access
WLAN or Wi-Fi	Wireless local area network

Glossary

Capacity	The volume of data that can be transmitted over a mobile communications network at a given point in time
Commercial approach	Delivery of public safety mobile broadband over one or more mobile carrier networks
Coverage	The geographic area or population over which a mobile network can be accessed to a given standard (such as from within buildings or via a vehicle radio)
Dedicated approach	Delivery of public safety mobile broadband over a dedicated network only
Dedicated network	A Public Land Mobile Network that is built and operated specifically for the use of public safety agencies
Dedicated spectrum	Spectrum set aside for use on a dedicated public safety mobile broadband network
Delivery option	A specific way of delivering public safety mobile broadband (within a deployment approach)
Deployment approach	A broad way of delivering public safety mobile broadband, such as through a dedicated network, commercial network(s), or a combination (hybrid)
Geotype	A class of geographical areas that, for the purpose of quantitative analysis, is deemed to have certain characteristics relating to the demand and supply of PSMB
Hybrid approach	Delivery of public safety mobile broadband over some combination of dedicated network(s) and mobile carrier networks
Interoperability	The ability of public safety personnel in different agencies or jurisdictions to communicate over a mobile communications network
Land Mobile Radio	A type of mobile communications network that provides voice and narrowband data communications, usually for the exclusive use of public safety agencies

Mobile carrier network	A mobile broadband network, operated by a commercial entity, that delivers services to retail customers
Mobile communications network	Any communications network where permanent infrastructure has been deployed to allow users to wirelessly send and receive voice or data communications
Mobile Virtual Network Operator	A company that resells services from mobile carriers directly to consumers
Network accessibility	The ability of users to establish a connection to a mobile communications network, even when it is congested
Overflow	The ability for public safety mobile traffic to be carried over a mobile carrier network once the capacity of a dedicated network has been reached
Prioritisation	The ability to give some voice or data traffic preference over other traffic
Public Land Mobile Network	Any mobile communications network under the control of a single operator
Public safety mobile broadband	Mobile broadband services that meet specific capacity, coverage and quality of service standards for public safety
Radio	Any device that can wirelessly send and receive information over a mobile communications network
Resilience/ reliability	The ability of a mobile communications network to provide and maintain an acceptable level of service, including in adverse circumstances
Ruggedise	To make end-user devices resistant to heat, pressure or water
Security	The prevention and/or rectification of disruption and interception of communications over a network
Spectrum	Radiofrequency spectrum used to transmit and receive information over a mobile communications network
Standalone network	A communications network that is not integrated with any other network

OVERVIEW

Key points

- Public safety mobile broadband (PSMB) holds considerable potential to improve how the police, fire, ambulance and other public safety agencies (PSAs) deliver their services. It will allow frontline officers to access high-speed video, images, location tracking and much more.
- PSAs currently rely on their own radio networks for voice communications and some low-speed data. Mobile broadband use has been modest due to concerns that the quality of commercial services is insufficient to support 'mission critical' operations.
- The network capacity that PSAs require is uncertain. PSAs are seeking a higher quality of service than what is currently available on commercial networks. However, the standards required (in terms of coverage, reliability, security, priority access and so on) are not specific.
- There are many ways to provide a PSMB capability, including the construction of a dedicated network, a commercial approach, or some combination (hybrid) of the two.
  - A dedicated network would give PSAs access to (and control over) their own PSMB network using their own parcel of spectrum.
  - A commercial approach would mean that PSAs obtain PSMB services from one or more of the commercial mobile carriers through a contract for service.
- The Commission has undertaken an illustrative evaluation of the costs of several specific delivery options over a 20-year period. The cost of a dedicated network was estimated to be in the order of $6.1 billion, compared to $2.1 billion for a commercial option. Even the lowest-cost hybrid option is twice as expensive as a commercial option.
- A commercial option is cheaper because it requires significantly less 'new investment' than a dedicated or hybrid option as considerable existing infrastructure could be used or shared.
- Risk factors also influence the relative merits of different options.
  - A dedicated network would likely take longer to deliver and offer less flexibility to scale up network capacity in the short term, relative to other options.
  - Providing priority services under commercial or hybrid options would be more technically complex than under a dedicated option. There are also commercial risks arising from limited competition and supplier 'lock-in'.
- The benefits of each option are not expected to vary markedly, since the options under evaluation have been designed to deliver a similar level of PSMB capability. On that basis, the cost evaluation is likely to provide the best guide to net community benefit for each option.
- On first principles, a commercial approach represents the most efficient, effective and economical way of delivering a PSMB capability to PSAs.
- Small-scale trials would provide an opportunity for jurisdictions to gain confidence in a commercial approach; gauge the costs, benefits and risks of PSMB; and develop a business case for a wider-scale roll out.
- Competitive procurement is essential. Splitting up tenders, leveraging infrastructure assets and insisting on open technology standards can help governments secure value for money.
- Achieving interoperability will require jurisdictions to agree on common technical standards. PSAs will also need to adapt their operations to make the most of PSMB. This includes protocols for sharing information and network capacity among agencies.
- Spectrum allocation is an Australian Government responsibility. Any spectrum made available for PSMB should be priced at its opportunity cost to support its efficient use.

Overview

Police, fire, ambulance and other emergency services (collectively 'public safety agencies', or PSAs) currently rely on their own land mobile radio (LMR) networks for most of their communications. These networks deliver voice and some data services, such as text messaging. They are reliable, resilient and secure, but they do not support high-speed data (such as video-based applications or the sharing of large files) and often they are not interoperable across agencies.

Mobile broadband technology opens up new ways for PSAs to access a vast range of information sources while in the field (such as video, images, location tracking and biometrics). This represents a significant opportunity to save lives and property, improve officer safety and drive productivity gains in the delivery of public safety. However, use of mobile broadband by PSAs is relatively modest compared to other sectors of the economy, and it is unlikely to increase significantly until a 'public safety grade' service is available.

What has the Commission been asked to do?

This study is about identifying — by way of a first principles analysis — the most efficient, effective and economical way of delivering a public safety grade mobile broadband capability to PSAs by 2020, giving consideration to:

- the need for the capability to be reliable and secure, nationally interoperable across jurisdictions and agencies, provide PSAs with priority access, and operate in both metropolitan and regional Australia
- the relative costs, benefits and risks of alternative options for deploying a public safety mobile broadband (PSMB) capability — including deploying a dedicated PSMB network, an approach that is reliant on commercial networks, or some combination of the two
- relevant domestic and international reports and experiences.

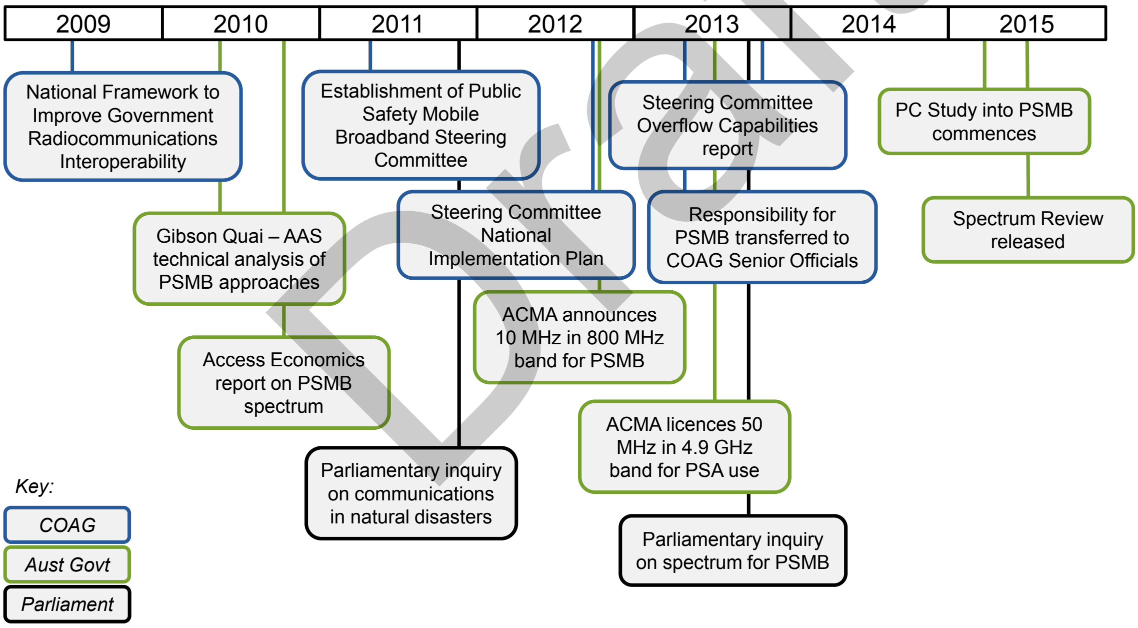
The Commission has not been asked to evaluate whether a PSMB capability should be delivered to PSAs — rather, the focus is on *how* best to deliver such a capability. The Commission's findings do not, therefore, answer the question of whether a PSMB capability is in the best interests of the community.

PSMB is not a new issue

This study is being undertaken in the context of earlier work relating to PSMB (figure 1). The Commission has drawn on these reports, which include work by state and territory governments and the Australian Government, done under the auspices of the Council of Australian Governments. The more substantive reports include:

- a detailed technical analysis of the costs of delivering PSMB under different options, commissioned by the Australian Government in 2010. Only limited parts of this analysis have been made public
- two reports produced by the Public Safety Mobile Broadband Steering Committee, which was established by the Australian Government in 2011 to consider the most effective and efficient way to deliver a PSMB capability. Neither of these reports has been released publicly.

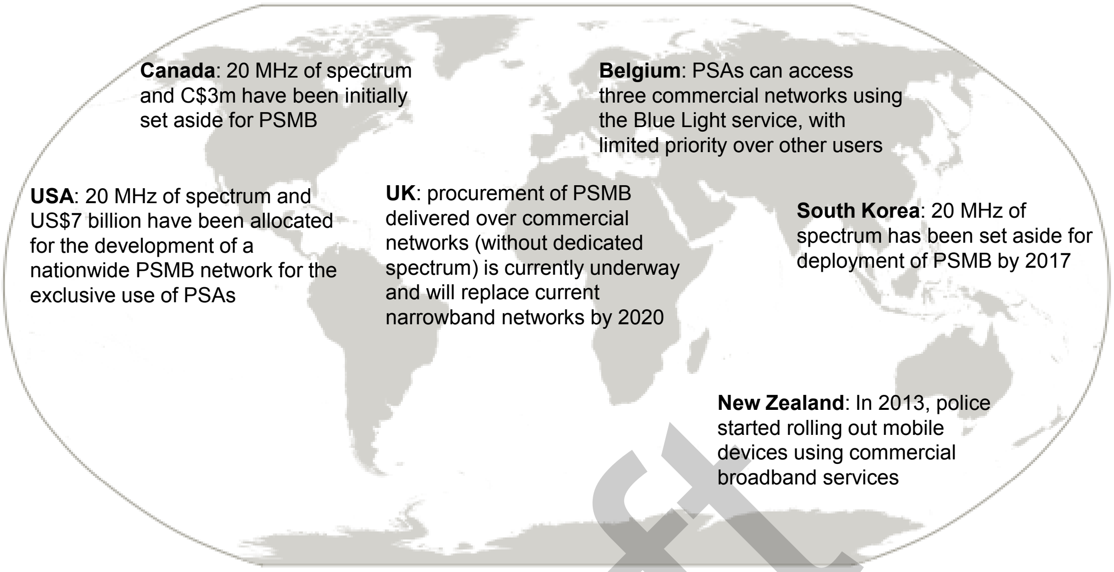
Figure 1 **Previous developments relating to PSMB**



Many countries are in a similar position to Australia

Several other countries are investigating, planning or implementing a PSMB capability. The specific approach taken differs across countries (figure 2). The United States, Canada and South Korea have announced that they intend to construct dedicated PSMB networks. By contrast, the United Kingdom and Belgium are pursuing commercial approaches to deliver PSMB.

Figure 2 **International approaches**



The communication needs of PSAs

Voice is the primary means of communication

Historically, voice has comprised the bulk of PSA communications, alongside paging systems (which support one-way broadcasts) and narrowband (low-speed) data services such as computer aided dispatch and text messaging.

Voice, paging and narrowband data are all supported by different types of LMR networks. These networks are usually built for the exclusive (or dedicated) use of PSAs and are specifically designed to meet their needs. LMR networks have extensive coverage and have proven to be reliable over decades of operation.

However, LMR networks also have weaknesses, including that they are often not technically interoperable across agencies and jurisdictions. The shortcomings of non-interoperability were revealed in recent large-scale natural disasters where public safety officers found that their communications equipment did not function when they crossed a state border. Even where officers are co-located, agencies have found it difficult or impossible to share information in the field (or have needed expensive network bridging equipment to do so). These experiences have led to repeated calls for interoperable communications systems.

Mobile broadband offers significant potential benefits

Public safety operations are increasingly dependent on information and the communication needs of PSAs are evolving accordingly. Even though mobile broadband technology is in its infancy, PSAs are already using mobile broadband applications in some areas and relying on commercial mobile networks to do so (box 1).

Box 1 How are PSAs using mobile broadband applications?

Fire and Rescue NSW is using mobile broadband for:

- Automatic Vehicle Location services, which can facilitate faster vehicle dispatch
- a 'First Responder' in-vehicle tablet application that provides officers with in-field intelligence and remote access to operating guidelines and databases
- in-vehicle applications for voice and video communications and inventory checks.

Victoria Police is using a mobile application that simplifies family violence reporting processes. It allows officers to pre-populate reporting forms with data already captured and stored in databases. As information is entered into the reporting forms, the relevant database entry is updated instantaneously.

The Ambulance Service of NSW uses mobile broadband to check and update electronic patient records in transit. This reduces the time spent on administrative tasks and enhances the quality of services delivered to patients.

Greater use of mobile broadband by PSAs could fundamentally change how they deliver their services, especially in 'mission critical' situations (box 2). The prospective benefits in terms of cost savings and improved public safety outcomes (such as lives saved or injury and property damage avoided) are manifold.

- The ability for ambulance officers to remotely access medical records or send images to the hospital could speed up treatment and save lives.
- Giving police officers the ability to access databases when in the field, and to collect and transmit key evidence, can significantly reduce time spent on administrative tasks.
- Providing firefighters with access to maps, building plans and locations of hazardous materials can help them locate incidents more quickly and identify how best to respond.
- More effective information sharing between agencies and the community can improve the situational awareness of public safety officers and the preparedness of community members.

Box 2 What is 'mission critical'?

The term 'mission critical' has many meanings. For example, a mission critical situation could refer to PSA activities or operations where reliable communications are necessary to avoid loss of life, serious injury or significant damage to valuable or strategic assets.

Alternatively, mission critical is used to describe certain properties of communications systems (such as resilience, priority and security) that make them fit for purpose in PSA operations. What is meant by a mission critical land mobile radio *voice* network is relatively well accepted. However, there is less clarity about what is implied by a mission critical mobile broadband *data* network.

For this study, the Commission has used 'mission critical' to refer to public safety activities or situations where lives are on the line (that is, where there is a material risk of loss of life or severe injury).

However, PSA uptake of mobile applications has been modest and piecemeal to date. This reflects concerns about the quality of service offered by commercial mobile carriers — Telstra, Optus and Vodafone (box 3). Critical issues include the ability of PSAs to get priority access to — and sufficient capacity on — commercial networks during times of congestion and the reliability of commercial networks relative to LMR networks. The consensus among participants is that PSAs are unlikely to make significant investments in, or widespread use of, mobile broadband until this occurs.

Box 3 Mobile broadband service quality has many dimensions

A number of dimensions (or characteristics) of mobile broadband service quality are important to PSAs.

- Accessibility — the ability of PSAs to get on to a mobile network, even when it is congested.
- User prioritisation — systems that prioritise certain PSA users, devices or applications over other mobile traffic on a network.
- Network coverage — the percentage of the population that resides in the coverage area, or the land area or road distance covered by a network.
- Network reliability (or resilience) — the ability of the network to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation. Reliability is often measured in terms of availability or network recovery time.
- Security — the techniques, strategies and infrastructure that are in place to uphold the confidentiality and continuity of communications.
- Interoperability — the ability of users to communicate by terminal device with whomever they need, when they need, when authorised.
- Device compatibility — the ability of officers to access mobile broadband using a wide range of field equipment (such as handsets or in-vehicle devices).
- Voice integration — the ability of mobile broadband networks to integrate and deliver the voice services that PSAs rely on.

Delivering a PSMB capability

The delivery of a PSMB capability relies on action by governments, PSAs and mobile carriers, regardless of the deployment approach. Without all of these entities playing their role, a PSMB capability is likely to be less efficient (and deliver fewer benefits) than it otherwise would, or may not eventuate at all.

State and territory governments have primary responsibility for public safety

Responsibility for public safety and emergency management mainly rests with state and territory governments. They have discretion to set their own policy agenda, along with the accompanying institutional arrangements and budget appropriation decisions as to whether and how to deploy a PSMB capability.

State and territory governments could become actively involved in facilitating PSMB in a number of ways. For example, they could:

- directly fund, own and/or operate a dedicated PSMB network
- pay one or more mobile carriers to deliver a PSMB service
- provide additional funding or other inputs to PSAs that would help them to build or purchase a mobile broadband service
- collaborate and coordinate efforts with other jurisdictions to develop technical standards and platforms for interoperability.

The Australian Government has a limited role

The Australian Government has a national leadership and coordination role in regard to emergency management and national security. It also directly funds the Australian Federal Police, the Australian Maritime Safety Agency, and some other PSAs. The Australian Government faces similar choices to the states and territories in terms of whether and how it facilitates a PSMB capability for these agencies.

The Australian Government is also responsible for the regulation and allocation of radiofrequency spectrum (a key input to mobile networks) and the economic and technical regulation of telecommunications services and infrastructure. These policy and regulatory levers could potentially be used to help facilitate the delivery of a PSMB capability.

For example, some study participants have suggested that the Australian Government (through the Australian Communications and Media Authority (ACMA), the agency responsible for regulating, licensing and pricing radiofrequency spectrum in Australia) should intervene to allocate spectrum to the states and territories *at a discounted price* for public safety purposes. Others have proposed that regulation be imposed on mobile carriers to facilitate the delivery of PSMB.

The Commission does not consider that there is a strong case for any material changes to the design or administration of existing regulatory regimes for the purposes of supporting a PSMB capability. Delivering a PSMB capability is not contingent on regulatory change.

Action by PSAs is crucial to the success of PSMB

The delivery and success of PSMB directly depends upon the actions of the agencies themselves, irrespective of how it is delivered. As users, PSAs are best placed to identify and demonstrate why government (taxpayer) support to facilitate a PSMB capability is in the best interests of the community as a whole. This means documenting how such a capability would be used to modify or enhance public safety operations, and how this translates into benefits for the community.

Once available, it is up to individual agencies to ensure that the capability is used efficiently. This will require a substantial shift in the mentality of how agencies collaborate and operate, especially in terms of sharing information and network capacity. It includes coming to agreement on how different agencies and officers will be prioritised over a network. Officer education and training, and revision of operational protocols, will also be required.

Delivering a PSMB capability has costs that will ultimately be met by taxpayers. It is important that PSAs (or entities acting on their behalf) are held accountable for any public funds used for PSMB. Moreover, ongoing public funding for PSMB should be contingent on clear evidence that the benefits justify the costs. Monitoring and reporting frameworks, established by state and territory governments, can support this.

Commercial carriers are part of the solution

Mobile network infrastructure is extensive, costly and in many cases long lived. There will be significant economies of scale and scope in using existing commercial infrastructure to deliver a PSMB capability, where this is technically and economically feasible. This means drawing on the extensive mobile networks already in place (Telstra, Optus and Vodafone each have a network covering upwards of 95 per cent of the population), as well as infrastructure owned by states and territories.

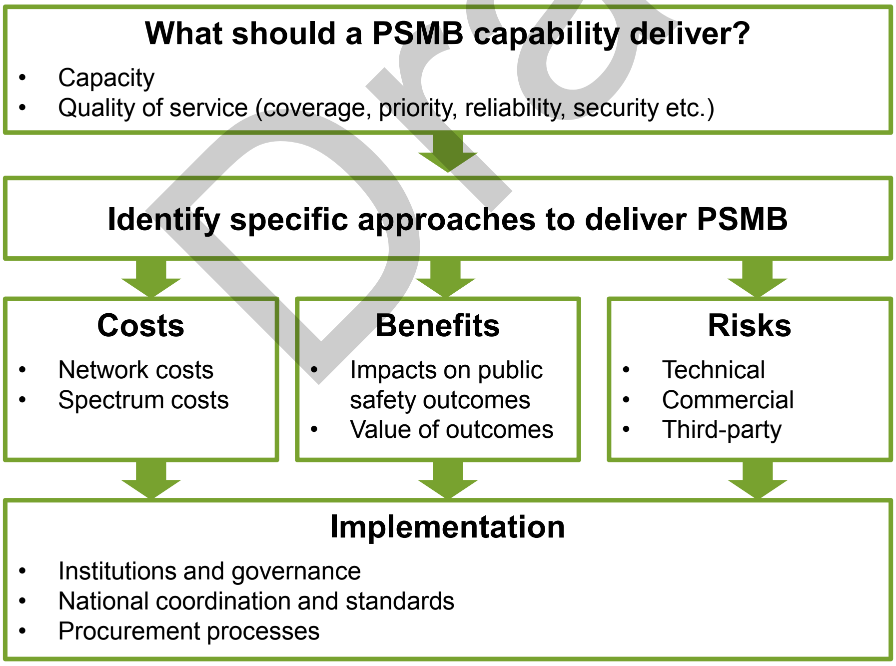
Mobile carriers also have considerable skills and expertise in network design and operation that could be brought to bear on a PSMB capability. Some have already taken an active role in putting forward solutions to meet public safety needs — for example, Telstra has demonstrated a capability called LANES that is designed to give priority services to PSAs.

The Commission's approach — a 'first principles' analysis

The Commission has undertaken a 'first principles' analysis to determine the best way to deliver a PSMB capability. The analysis has involved (figure 3):

- understanding the mobile broadband requirements of PSAs, taking into account the mission critical nature of public safety work and the service quality requirements this gives rise to
- identifying options that could feasibly meet these requirements, including a dedicated PSMB network, an option reliant on commercial networks, and hybrid options
- evaluating the costs, benefits and risks of each option, from the perspective of the community as a whole
- considering the implementation challenges and risks associated with PSMB and strategies to overcome these.

Figure 3 **The Commission's framework**



Where possible, the costs of alternative PSMB options have been evaluated in a quantitative way, using a network costing approach. This has helped to identify the relative importance of particular cost drivers and the magnitude of specific tradeoffs. However, data limitations mean that the benefits and risks of each option cannot be quantified in monetary terms.

In effect, the Commission has undertaken a cost-effectiveness analysis and supplemented this where feasible with a qualitative analysis of the benefits and risks of different delivery options. That said, as the options under evaluation have been designed to deliver a similar level of PSMB capability, the impact of each option on public safety outcomes (and thus its benefits) is not expected to vary markedly.

A key output of the Commission's analysis is a set of principles that would deliver a PSMB capability in a way that is efficient, effective and economical.

What should a PSMB capability deliver?

A PSMB capability can be described in terms of the amount of network *capacity* that is available to end users (for example, in terms of megabits per second) and the *quality* of services delivered (box 3).

PSA demand for network capacity is uncertain

There is widespread agreement among participants and other stakeholders that PSA use of mobile broadband would increase significantly if a public safety grade service were available — particularly in terms of uplink traffic (that is, sending data from the field), and largely driven by video-based applications.

However, detailed information about how PSAs would use a PSMB capability (including the type, composition and volume of mobile applications), and what this implies for PSA demand for network capacity, is lacking — as is information in the public domain on the benefits of that use. Similarly, while many participants pointed to the importance of a PSMB capability providing 'sufficient' network capacity, evidence on what this means for the quantum of network capacity is sparse.

There are valid reasons for this. PSA demand for public safety grade mobile broadband services will depend on a complex range of factors, including the pricing model and prices that PSAs face, the availability of alternative communications systems (including LMR, Wi-Fi and satellite), PSA procedures and protocols for broadband use and prioritisation and technological developments. All of these factors are largely unknown or at a nascent stage of development.

The Commission has thus made a number of assumptions about the level of network capacity that a PSMB capability could deliver, in order to undertake the quantitative analysis. These assumptions are illustrative only. They are not suggestive of the level of network capacity that jurisdictions should adopt or of PSA demand for mobile broadband.

PSMB must support mission critical operations

While not all PSA activity is mission critical (such as routine or administrative tasks that may be considered operational, informational or business critical), it is not practical to offer PSAs a 'two-tiered service'. Mission critical situations are difficult to predict in advance and situations can rapidly escalate to mission critical as circumstances change. For these reasons, PSAs require that their communications systems have the capacity to be used in mission critical situations as a matter of course.

Delivering mission critical voice services over PSMB will take time

It is too early to consider delivering mission critical *voice* services (such as 'push to talk' and 'group calling' applications) over a PSMB network, regardless of the deployment approach. International standards and applications for these services are still being developed, and it will take time to design, test and prove fit-for-purpose handsets and software. Even once these issues are resolved, the case for migrating voice services will depend on a range of other factors, including the lifespan of LMR networks and availability of commercial offerings.

All Australian jurisdictions plan to continue operating their LMR networks until at least 2020, and the Queensland Government recently invested over $450 million in its Government Radio Network, which is expected to operate until 2029. In the meantime, however, it is important that the design and implementation of PSMB networks is compatible with the prospect of integrating mission critical voice services at a later date.

Operationalising the concept of a mission critical data network is difficult

What is meant by a mission critical LMR voice network is relatively well accepted (although not necessarily universally defined). However, what is implied by a mission critical mobile broadband data network is less clear. Participants provided little detail about the specific levels of service that are sought, or the way in which the quality characteristics important to PSAs (such as security or 'guaranteed' network access) should be met. Drawing on insights from the limited international experiences of implementing a PSMB capability, the Commission has proposed a starting point definition for service quality.

Specifically:

- the network should be available 99.9 per cent of the time, and cover at least 99 per cent of the population
- PSAs should be provided with priority access to (and capacity on) PSMB networks, with scope to change these arrangements in real time
- PSAs should be able to communicate with each other (within and across jurisdictions) and access PSMB networks upon crossing jurisdictional borders

- communications over a PSMB network should be secure (for example, through end-to-end encryption).

The Commission is seeking feedback on how the concept of a mission critical data network should be operationalised ahead of the final report.

Demand management is crucial to getting the most out of PSMB

PSAs' activities — and their corresponding communications needs — can be broadly classified into 'business as usual' periods and peak periods. Peak periods refer to times where PSAs are responding to major or emergency incidents (a natural disaster or hostage situation) or large planned events (such as New Year's Eve or the Melbourne Cup) in addition to business as usual.

Many peak demand periods for PSAs are unpredictable in timing, location, severity and incidence (as is the nature of crisis and emergency). Moreover, PSA communications increase significantly (and by as much as ten- or twenty-fold) during peak periods compared to 'business as usual' periods. A PSMB capability that caters for relatively infrequent peak events would be very expensive, as it would lead to low levels of capacity utilisation (figure 4) and high marginal costs per megabyte of data transmitted.

Dimensioning a mobile network to meet lower levels of demand does not necessarily mean that PSMB networks would be severely congested during major incidents, or that important demand would go unmet. Indeed, not all PSA demand needs to be met in real time. Strategies to reduce PSA demand during peak periods — such as through 'store and forward' or 'compression and broadcast' of video-based applications or offloading traffic to alternative networks (fixed or Wi-Fi) — are crucial to ensuring the net benefits of a PSMB capability are maximised.

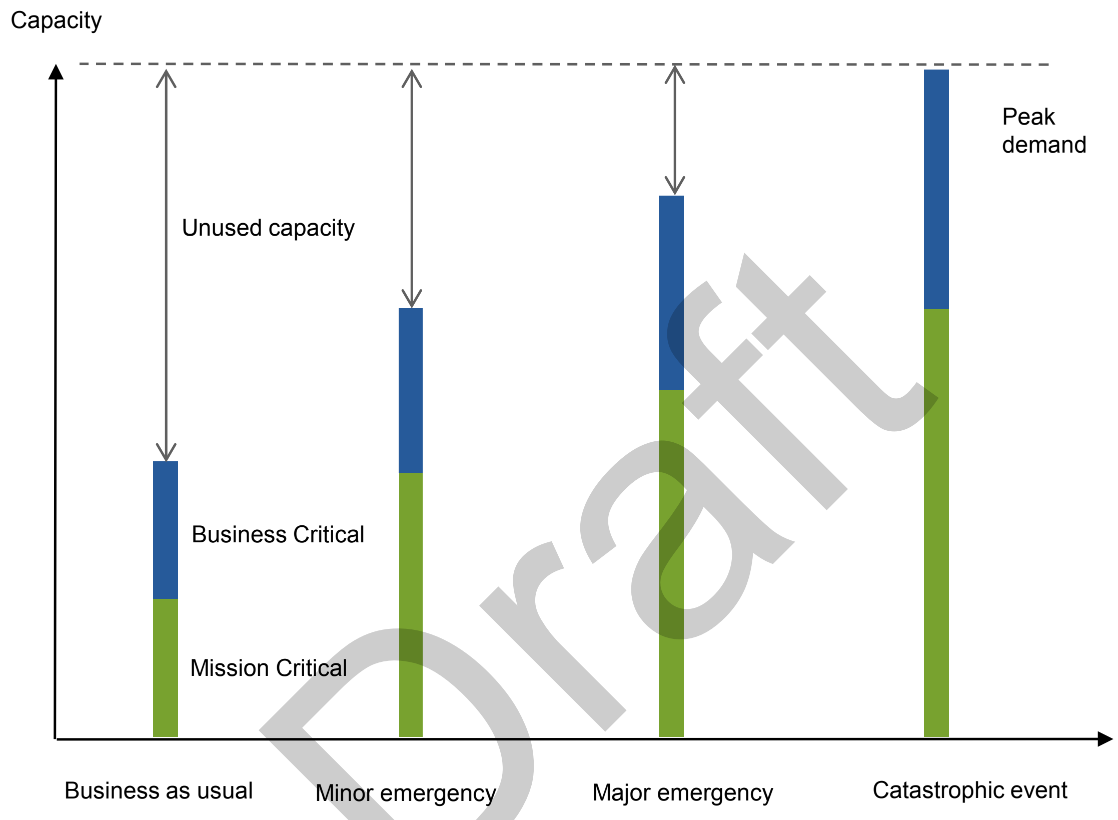
Efficiency should be the guiding objective

There is no single definition of a public safety grade mobile broadband capability — a range of capacity levels and service quality standards could feasibly apply. However, delivering a PSMB capability has costs, and many of these costs (met by governments and ultimately taxpayers) increase exponentially with capacity and service standards.

It is in the best interests of the community for individual jurisdictions to pursue a capability that reflects their particular needs and circumstances as well as their communities' willingness to pay for public safety grade mobile broadband services. Given their varying circumstances, it is unlikely to be efficient for each jurisdiction to pursue the same approach at the same time. This highlights the importance of identifying a flexible pathway and framework for the delivery of a PSMB capability.

A key consideration for all jurisdictions is how the capability should be delivered. Different approaches give rise to potentially different costs, benefits and risks. These need to be evaluated and weighed up to determine the best way forward.

Figure 4 **Meeting peak demand implies significant network capacity**



How should a PSMB capability be delivered?

There are many possible delivery options

There are myriad combinations of technologies and infrastructure that could feasibly be deployed to deliver a PSMB capability.

With regard to technology, there is widespread agreement — both internationally and among participants — that PSMB should be delivered using 4G Long Term Evolution (LTE) technology (with open standards to provide scope for future upgrades), regardless of the deployment approach chosen. It has advantages over previous mobile technologies (such as increased peak data rates, higher spectral efficiency, and the ability to automatically detect and rectify faults), and will continue to evolve and improve.

However, there are varied and strong views about whether, and to what extent, the infrastructure embodied in a PSMB capability (such as a core network, base stations and associated equipment, backhaul capacity and radiofrequency spectrum) should be dedicated to PSA users, or shared by PSAs and other users as part of a commercial solution. While it is technically feasible to deliver a PSMB capability under a dedicated, commercial or hybrid approach, the costs and risks can vary significantly.

A number of options have been evaluated

The Commission has evaluated four specific options (and variants thereof) for delivering a PSMB capability in areas of Australia where there is existing commercial mobile coverage (table 1). The analysis assumes that PSMB is rolled out nationally, although the implications of taking a state-by-state approach have also been examined. The Commission has also considered the costs of delivering a PSMB capability in areas of Australia where there is currently no commercial mobile coverage, but there is LMR coverage (box 4).

Table 1 **Overview of PSMB delivery options evaluated**
Areas within commercial carrier coverage footprints

	Dedicated spectrum for PSAs	*Coverage in dense urban, urban and suburban areas*	*Coverage in rural and remote areas*	*Number of networks involved*
Option 1 (dedicated)	Yes	Dedicated	Dedicated	1
Option 2a (hybrid)	Yes	Dedicated and commercial	Dedicated and commercial	1
Option 2b (hybrid)	Yes	Dedicated and commercial	Dedicated and commercial	2
Option 2c (hybrid)	Yes	Dedicated and commercial	Dedicated and commercial	3
Option 3a (hybrid)	Yes	Dedicated and commercial	Commercial	1
Option 3b (hybrid)	Yes	Dedicated and commercial	Commercial	2
Option 3c (hybrid)	Yes	Dedicated and commercial	Commercial	3
Option 4a (commercial)	No	Commercial	Commercial	1
Option 4b (commercial)	No	Commercial	Commercial	2

Box 4 **Deploying a PSMB capability outside the commercial footprint is very expensive**

Some areas of Australia do not have commercial mobile coverage at present, but are covered by land mobile radio networks. Because there is limited scope to use existing infrastructure in these areas, the cost of rolling out a permanent LTE network would be very high. It would require substantial investment in new base station sites and backhaul capacity. The cost of building a new base station site is in the order of three to seven times more expensive (according to some estimates) than deploying new equipment to an existing base station. The benefits of a permanent mobile network in these areas would need to be extremely large to justify the costs. That said, it is possible that targeted, small-scale network extensions may be warranted in some cases.

There are lower cost options (such as transportable base station equipment, or satellite broadband) that can be pursued to provide a level of mobile broadband coverage and capacity in these areas, albeit not to a public safety grade. Commercial mobile carriers and land mobile radio network operators already use these techniques in areas without permanent mobile broadband coverage.

A dedicated PSMB capability (option 1)

A dedicated PSMB capability would mean that PSAs have access to (and control over) their own PSMB network, using their own parcel of spectrum. While it is assumed that existing sites and backhaul would be used as part of this solution, significant new investment would be required. This includes new base stations, base station equipment, backhaul capacity and core networks (control centres).

PSAs would not be able to ‘overflow’ onto commercial networks for public safety grade mobile broadband services under this option. However, they would be able to purchase standard commercial mobile services, as they do today.

A commercial approach (option 4)

A commercial approach would mean that PSAs obtain PSMB services from one or more commercial mobile carriers through a contract for service. Carriers would determine how best to meet PSA requirements using their own mobile networks and spectrum holdings.

This option would require that commercial carriers harden their networks to improve network reliability. This could include installing additional battery backup, upgrading physical sites and building new backhaul links. Adding PSA traffic to carrier networks would also be expected to bring forward investments in sites, spectrum and backhaul.

A commercial approach could involve one or multiple mobile carriers. Both possibilities have been evaluated.

A full coverage hybrid approach (option 2)

A full coverage hybrid approach would provide PSAs with a dedicated network that covers the entire commercial mobile footprint (as per the dedicated approach) and their own parcel of spectrum. PSAs would also be able to use one or more commercial carrier networks to access additional public safety grade network capacity on a preferential basis.

What is implied by a ‘dedicated network’ under this option can vary. On the one hand, PSAs could rely on the core network of a mobile carrier (that is, the core network is shared). However, the parcel of spectrum set aside for PSAs under this option would *not* be shared, meaning PSAs would still have access to their own dedicated ‘channel’. This would be sufficient for some (but not all) of PSAs’ capacity needs.

Alternatively, the dedicated network could be supported by a separate core network built for PSMB, which would interface with one or more carrier networks. The potential advantage of a separate core network is that it would provide PSAs with more control over the configuration and operation of the dedicated network. For example, relative to sharing a core network, this approach may be more amenable to PSAs (or an agent on their behalf) directly managing the prioritisation of public safety officers in real time.

Both alternatives have been considered as part of the Commission’s analysis, as has the option of relying on multiple mobile carriers to deliver the commercial component of this delivery option.

A partial coverage hybrid approach (option 3)

A partial coverage hybrid approach would provide PSAs with a dedicated network that covers metropolitan areas only (defined as dense urban, urban and suburban areas, which contain over 80 per cent of the population), and their own parcel of spectrum.

PSAs would rely on commercial carrier networks for some of their capacity needs in metropolitan areas (once they exhaust their own dedicated capacity). Outside of the metropolitan region, PSAs would rely on commercial carriers for both coverage and capacity.

As with the full coverage hybrid approach, PSAs could rely on the core network of a single mobile carrier, or could establish a separate core network built for PSMB, which would interface with one or more commercial carrier networks. Both alternatives have been considered as part of the Commission’s analysis.

Costs have been assessed using a network costing approach

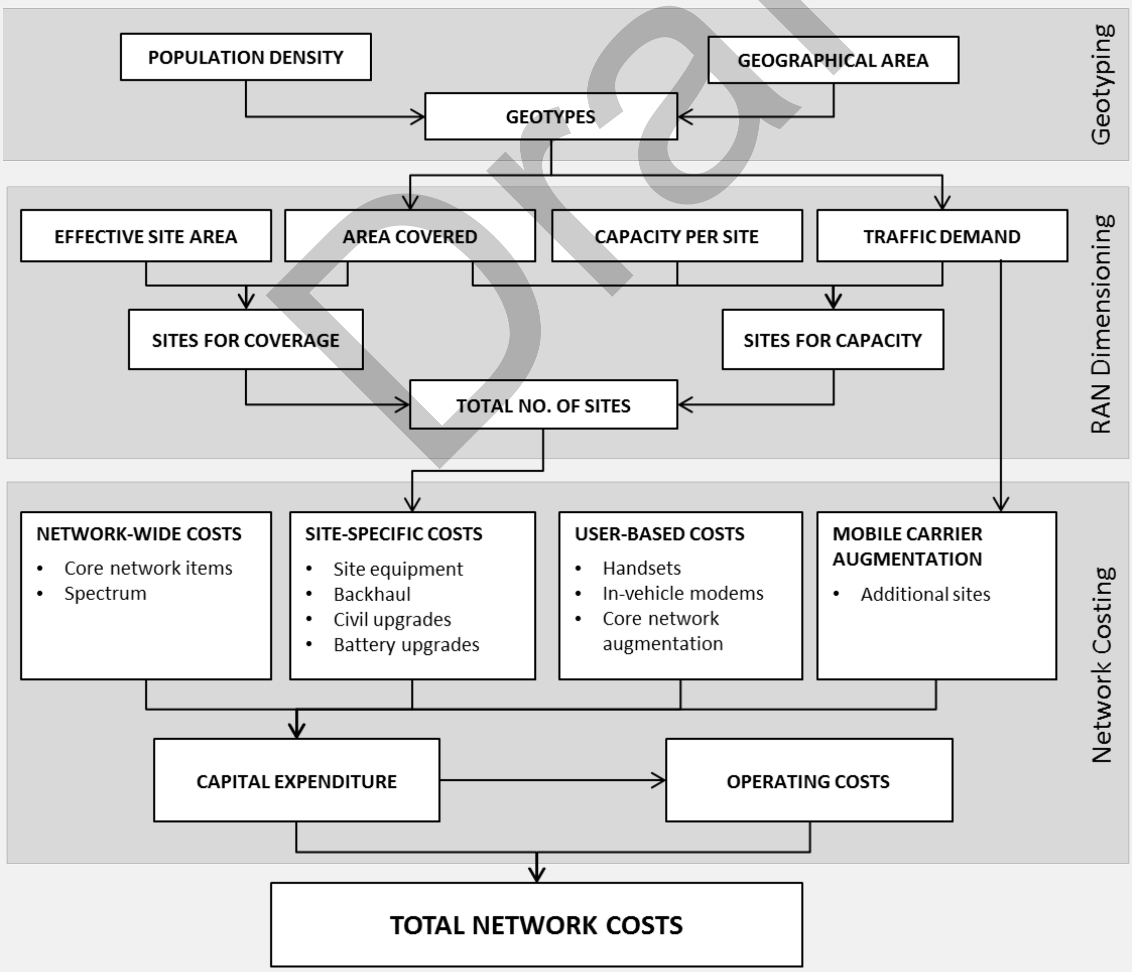
The Commission has assessed network costs in a quantitative way, using a fit-for purpose, bottom-up approach (box 5). The framework and methodology draws on that used in other analyses but is adapted to the specific nature of this study.

Box 5 A 'fit for purpose' framework for evaluating network costs

The bottom-up cost framework involves three key steps, as illustrated below.

- Geotyping — using census data to assign different geographical areas of Australia to particular geotypes (dense urban, urban, suburban, rural or remote).
- Radio access network dimensioning — estimating the number of mobile sites required to meet the coverage and capacity requirements embodied in the PSMB scenarios.
- Network costing — applying benchmark cost values (such as the costs of mobile base station equipment) to calculate total capital and operating costs.

The key output from the quantitative evaluation is a net present value for each option, assuming a 20 year time horizon (over the period 2018 to 2037).



The primary objective of the quantitative analysis is to identify indicative cost differences between different options for delivering a PSMB capability, and the key drivers of those cost differences. It is not designed to:

- produce precise estimates of the total costs of individual options or individual cost components
- describe what the architecture of a PSMB network would look like in practice
- calculate the optimal mix of inputs for delivering a PSMB capability.

The cost analysis focuses on estimating the incremental (rather than total) opportunity costs associated with each PSMB delivery option — that is, the value of the next best alternative use of these resources. The focus is not on the distribution of costs or the prices for PSMB communication services that might be charged in practice.

To compare costs on an even keel, it is assumed that each option would deliver the same level of PSMB network capacity, as defined by the Commission's capacity assumptions (discussed above). Dealing with the quality dimension of a PSMB capability is more difficult. While the Commission has proposed a starting point definition of mission critical mobile data standards, the options evaluated in this report are not explicitly designed to meet all of these standards. This reflects limited and conflicting evidence as to whether and what technologies and infrastructure could be put in place to achieve the specified standards.

Nevertheless, certain levels of service quality are implied by the assumptions made in the quantitative analysis, and are common to all options. Specifically, under each option:

- the network has been designed to provide geographical coverage equal to existing commercial networks, which equates to a population coverage in excess of 99 per cent
- some capital investment is made to the core network to provide priority services to PSAs
- a proportion of network sites are subject to some form of hardening, which is assumed to improve network resilience and reliability.

There is a lack of publicly available information to inform some of the key assumptions and parameters used in the quantitative evaluation. In these cases, a preliminary judgment has been made for the draft report and the robustness of the results has been subject to sensitivity testing. Feedback is sought on the assumptions and parameters used in the quantitative evaluation to inform the final report.

The costs and risks of delivery options vary markedly

A commercial approach minimises costs

The Commission's quantitative analysis found that deploying a dedicated PSMB capability is nearly 3 times more expensive than relying on commercial networks. Specifically, the estimated net present cost of the dedicated option over 20 years is about $6.1 billion, compared with about $2.1 billion for a commercial option (table 2).

Table 2 **Composition of PSMB delivery costs**

Cost item	*Dedicated*	*Hybrid*		*Commercial*	
		Minimum (option 3a)	Maximum (option 2c)[a]	Minimum (option 4a)	Maximum (option 4b)
	$m	$m	$m	$m	$m
Radio access network equipment	1 150	692	1 048	..	..
Hardening	174	164	123	117	92
Core network and add-ons	143	42	1 190	42	84
User equipment	532	532	532	532	532
Mobile carrier network augmentation	..	52	52	251	251
Spectrum	264	224	264	..	..
Operating costs	3 857	2 627	3 989	1 140	1 146
Total cost[b]	**6 123**	**4 335**	**7 201**	**2 083**	**2 107**

[a] Assuming a state-by-state rollout. [b] Figures may not add due to rounding. **..** Not applicable.

The cost difference between the commercial and hybrid options narrows as the geographic region covered by the dedicated component decreases, and as the extent of infrastructure (core network) sharing increases.

However, even the lowest-cost hybrid option considered by the Commission (option 3a) is estimated to be twice as expensive as a commercial network option ($4.3 billion compared to $2.1 billion). For this hybrid option, it is assumed that PSAs would share a core network with a commercial carrier, but public safety officers operating in metropolitan areas would be able to use a dedicated channel to meet some of their communications needs (approximately 80 per cent of total demand). Outside of this, PSMB services would be delivered by commercial carriers using their infrastructure and spectrum.

There are two main reasons why the cost of delivering a PSMB capability is estimated to be lower under a commercial option, relative to a dedicated or hybrid approach.

- The dedicated option (and to a lesser extent, the hybrid options) requires significantly more new investment. This includes new sites, base station equipment (to operationalise the dedicated spectrum), a core network and backhaul.

- Commercial carriers have a wider portfolio of spectrum resources, providing them with greater flexibility to meet customer requirements at least cost.

Further, commercial carriers are expected to be able to minimise PSMB operating costs by spreading certain costs (such as the costs associated with maintaining base station site equipment) over a larger number of users. It has not been possible to model these efficiencies due to data limitations. However, the input assumptions used in the quantitative analysis have been adjusted so that operating costs are lower under a commercial option.

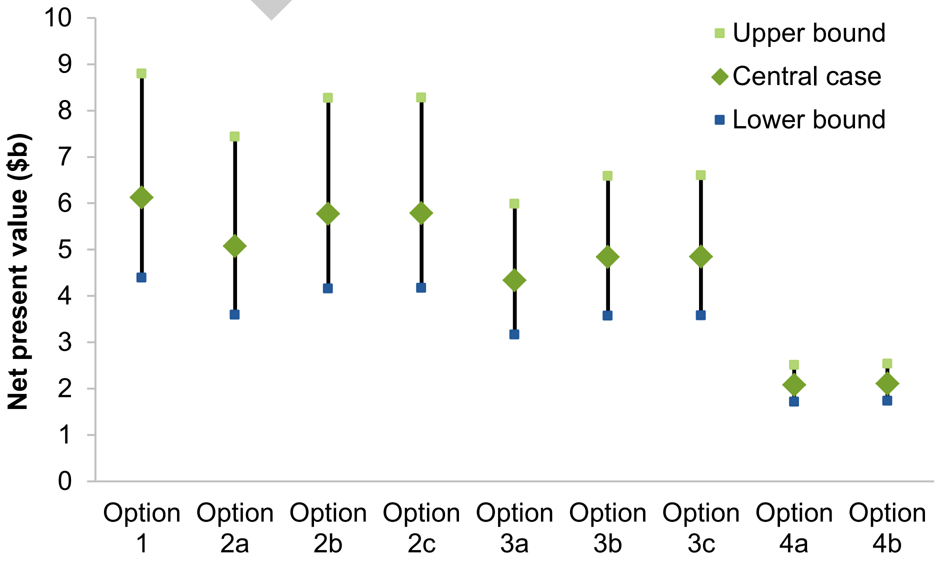
Sensitivity analysis has been used to understand how changes to different variables and assumptions (particularly those where there is a high degree of uncertainty) affect overall costs.

The results are most sensitive to assumptions about the level of capacity the network is dimensioned to provide (and how this changes over time), backhaul leasing charges, site equipment costs and site leasing charges. Other parameters (such as the cost of building new sites) have less bearing on the cost estimates.

Importantly, varying key assumptions and input values simultaneously to explore 'best case' and 'worst case' scenarios does not change the rankings of the different options — the commercial option remains the lowest cost option under all of the scenarios evaluated (figure 5). For example, a dedicated network is estimated to be between about 2½ and 3½ times more expensive than a commercial option, depending on the assumptions used.

Figure 5 **PSMB delivery costs**

Best case and worst case sensitivity analysis



Moreover, the estimated range of costs for the commercial option is small compared to the other options. This is because some input values that are only relevant to the dedicated and hybrid options are highly uncertain (such as site leasing and base station equipment costs), and so a wide range of values for these inputs has been considered in the sensitivity analysis.

Under a dedicated or hybrid option, a state-by-state approach would be significantly more costly than a national approach, primarily due to duplication of core networks and operating costs. For example, the cost of each state implementing a dedicated network is about 20 per cent more expensive than a national approach.

Other factors to consider

There are factors other than cost to consider when deciding which delivery option to adopt. Specifically, the risks associated with delivering PSMB can vary depending on the deployment approach, and so may bear on the relative merits of respective options. Deployment timeframes, the flexibility that options afford to governments and PSAs, and the potential impacts of PSMB on other mobile customers are also relevant.

Commercial and hybrid approaches are more susceptible to supplier lock-in

Supplier lock-in occurs when a customer is dependent on a single (or very few) supplier for a service, and is unable to change supplier without incurring significant switching costs.

Supplier lock-in can stem from a supplier using non-standardised technology (for example, when there is only one supplier of proprietary equipment). This risk is common to all PSMB delivery options and can usually be managed through contracting and procurement processes.

Lock-in can also arise as a result of significant and unrecoverable investments being made by a single supplier, making it difficult — and potentially very costly — for customers to switch suppliers in the future. This, in turn, can influence the pricing behaviour of the incumbent supplier. This risk is most pronounced under the commercial and (to a somewhat lesser extent) hybrid options, where it is assumed that a commercial carrier would undertake significant investment.

A multiple-carrier solution would be highly complex

Solutions which use multiple mobile carriers for service delivery can potentially spread investments over several networks. This may lower the risk of lock-in by reducing the amount of investment sunk into any one network, improving contestability for future PSMB contracts and upgrades. The use of multiple networks also creates a level of redundancy (or overlap between networks) that means less investment in hardening may be necessary to meet reliability requirements.

In practice, however, implementing a multiple-carrier solution would be complex. Networks would need to be linked to one another — and some coordination in technology upgrades may be required — to allow PSAs to roam from one carrier to another. This would require contracts to be negotiated between carriers covering technical settings and billing arrangements. It would also be commercially difficult, given the rarity of roaming agreements between carriers in Australia.

A dedicated option provides little flexibility to scale up capacity in the short term

A dedicated option provides almost no scope, at least in the short term, to accommodate an increase in demand beyond what the network is initially provisioned to meet (except by way of 'transportable' mobile cells, which take time to deploy once an incident is underway). While network capacity can be rationed to prioritise the most urgent communications, some important users or applications may inevitably need to be dropped.

In most parts of Australia, commercial networks have large amounts of capacity that could accommodate spikes in PSA communications during large-scale events. A commercial or hybrid approach therefore provides much more flexibility than a dedicated network — PSAs could agree to purchase a base-level of capacity with the option to exceed this amount should the situation require it.

It is technically possible to provide priority services for PSAs without dedicated spectrum (but it has not been demonstrated)

The need to provide PSAs with a parcel of dedicated spectrum (for their exclusive use) has been a contentious issue in this study. Some participants consider that network access and user prioritisation would be at risk if services were delivered using shared spectrum (that is, as part of a commercial solution) and favour a dedicated or hybrid approach on this basis.

However, evidence underpinning these arguments is sparse. By contrast, equipment vendors and technical experts have indicated that features of LTE technology mean that it is technically feasible to provide priority access and capacity to PSAs without dedicated spectrum.

That said, the ability (or willingness) of commercial carriers to provide these features without dedicated spectrum is yet to be demonstrated. Some elements of prioritisation technology have been demonstrated on a pilot basis (for example, access technology in Telstra's LANES product). However, many PSAs remain uncertain about the capability of the technology and have indicated a reluctance to rely on mobile broadband data services that are delivered using commercial carriers' spectrum.

Rollout timeframes and delay risks vary

A dedicated network is expected to take longer to deliver (and therefore longer for the associated benefits to be realised) than a hybrid or commercial approach because of the significant amount of capital investment required upfront.

A separate issue is the risk of delay to a rollout timetable once it has been set in place. Any delay in PSMB availability could reduce its benefits, as these will also be delayed. All options could face delays due to contract negotiation. However, the risk of delay is expected to be higher under a dedicated or hybrid approach as:

- spectrum may not become available until a formal spectrum allocation decision is made by ACMA, or could be dependent on ongoing international processes to agree on harmonised spectrum
- deploying new infrastructure and equipment takes time, and lengthy complex projects are more likely to overrun their expected delivery dates.

Technology upgrades might prove less economic under a dedicated approach

Commercial mobile networks are continually upgraded as mobile carriers make new investments to keep up with evolving technology and competitor offerings. Some of these upgrades have high fixed costs that are largely invariant to the number of users on the network.

The relatively small number of users on a dedicated PSMB network would mean that implementing future upgrades to technology (such as emerging 5G technologies) would come at a high cost per user. By contrast, mobile carriers have large user bases over which to recover these costs.

This could mean that new technologies are incorporated more slowly under a dedicated option (and to a lesser extent under the hybrid options) relative to the commercial option. This, in turn, could mean that parts of the PSMB network become incompatible with new applications and devices developed for consumer markets.

It is unclear whether (or how) non-PSA users would be affected under a commercial or hybrid option

Some participants have suggested that delivering a PSMB capability could have consequences for the quality of service experienced by other mobile users (where network infrastructure and spectrum is shared, such as under a commercial or hybrid approach).

On the one hand, enhancements to carrier networks to ensure that mobile services are delivered to a public safety standard could improve the quality of service experienced by non-PSA users (a positive spillover). On the other hand, providing PSAs with access and priority guarantees may mean displacing commercial customers or degrading their quality of service at certain points in time (a negative spillover).

It is impossible to know with any certainty whether carrier involvement in a PSMB capability would improve or worsen the quality of service experienced by non-PSA users overall. How these spillover effects would vary across the commercial and hybrid delivery options is also uncertain. In any case, these effects would likely be reflected in the prices charged by carriers (to both PSA and non-PSA users).

The way forward

A commercial solution offers the best way forward

On first principles, the most efficient, effective and economical way of delivering a PSMB capability to PSAs is by relying on commercial mobile networks (including spectrum), services and expertise. Relative to a hybrid or dedicated approach, a commercial approach:

- imposes a considerably lower cost on the community
- is expected to deliver a PSMB capability sooner, and carries a lower risk of delay
- provides PSAs with the flexibility to scale up demand in the short-term, where it is efficient to do so
- lowers the per user cost of adopting technology upgrades, increasing the likelihood that these upgrades are undertaken in a timely way.

A commercial approach does carry a higher risk of supplier lock-in. However, there is some scope to reduce this risk through good procurement processes and careful contracting (discussed later). Moreover, while lock-in risks are significantly reduced under a dedicated option, it is highly unlikely that the estimated $4 billion cost difference between these options is justified based on lock-in risk alone. Hybrid options with a small dedicated component are closer in cost to the commercial approach; however, these options do not significantly reduce the lock-in risk (given their heavy reliance on commercial networks).

Trials would provide an opportunity to develop confidence in a commercial approach

As noted earlier, there is considerable evidence to suggest that it is technically feasible for commercial carriers to deliver priority access for PSAs without dedicated spectrum. Given the additional costs involved, the Commission considers that the case for using dedicated spectrum to deliver PSMB (that is, a hybrid approach) is weak.

However, to the extent governments or PSAs have residual reservations about the capability of commercial carriers to deliver a public safety grade service using shared spectrum, this can be managed through small-scale trials or pilot programs that prove the technology. Only in the event that these attempts fail would it be appropriate to consider using dedicated spectrum to deliver PSMB services. Investing in dedicated spectrum in anticipation of commercial carriers failing to deliver the requisite services would represent a highly risk-averse and costly strategy.

The public safety sector is well placed to seek such assurances from the private sector. LMR voice networks will continue to be available for at least the next 5–10 years in all jurisdictions, creating a relatively low-risk environment for experimentation with new technology.

Undertaking trials (on short-term contracts and in targeted areas, for example) has other benefits, and may be advantageous even if jurisdictions are confident that the carriers can deliver PSMB without dedicated spectrum. Trials would help jurisdictions to better gauge the costs, benefits and risks of PSMB, and to identify risk mitigation strategies. Moreover, the outcomes and lessons from trials could be used to build a business case to expand the capability more widely. Indeed, starting small is likely to be beneficial for all jurisdictions, given the significant uncertainty about PSA demand for mobile broadband services and technological developments.

Spectrum should be priced at its opportunity cost

All mobile broadband networks require access to spectrum.

- Under a commercial approach to delivering PSMB, the spectrum holdings of commercial carriers would be used. A carrier might rely exclusively on its existing spectrum assets or purchase some new spectrum to accommodate PSA traffic.
- Under a dedicated or hybrid deployment approach, the relevant state or territory government would need to obtain the right to access a suitable band of spectrum.

In 2012, ACMA made an in-principle decision to set aside 10 MHz of spectrum within the 800 MHz band to support the deployment of a PSMB capability. A final decision on the allocation of this spectrum is yet to be made. However, any state or territory government that wishes to access spectrum for PSMB is not dependent on the outcome of this process — they can apply to ACMA for an apparatus licence, or obtain a spectrum licence (either at auction or from an existing licence holder).

Regardless of how and to whom spectrum is made available, it should be priced at its opportunity cost — the value of the next best use for the spectrum. This would give purchasers a strong incentive to use spectrum in an efficient way, including potentially leasing or selling spectrum access rights to a third party when it is not needed.

A flexible licensing approach that allows state and territories to purchase small and/or localised spectrum bands, potentially over a short time period, would give jurisdictions greater scope to trial a PSMB capability, such as by rolling out a dedicated network in particular areas. It could also be valuable for jurisdictions seeking to acquire spectrum resources to use as leverage in negotiations with commercial carriers.

Cost-reflective pricing would encourage efficient use of PSMB

Jurisdictions can facilitate the efficient use of PSMB (and efficient investment in it over time) by adopting cost-reflective pricing models. This would encourage agencies to consider the costs and benefits of using PSMB (against other inputs, such as vehicles and equipment) and give PSAs an incentive to manage their demand efficiently when networks are congested.

Where state or territory governments choose to assist PSAs with meeting the costs of using PSMB, this should be done in the form of an increased budget allocation. This would preserve the incentives PSAs have to use PSMB efficiently, relative to alternative funding models (such as directly subsidising the provision of PSMB or key inputs).

A statewide implementation entity could help

Regardless of how jurisdictions proceed, implementing a PSMB capability will involve a number of technical and commercial tasks, such as developing the technical specifications that a PSMB capability would need to meet, or directly procuring services.

There would be benefits in entrusting a dedicated agency in each jurisdiction to undertake such tasks. Some jurisdictions have already established agencies to manage PSA communications and invest in LMR networks at the state level (such as the NSW Telco Authority) and could potentially task these agencies with the implementation of a PSMB capability.

History suggests that a statewide approach is likely to be more effective than letting each PSA independently make procurement decisions. The latter approach has led to duplication of investments in LMR networks and significant constraints on technical interoperability across agencies in many jurisdictions. By contrast, a statewide approach could:

- minimise duplication of equipment and procurement
- lead to economies of scale (for example, where purchasing a larger number of handsets would reduce the unit cost)
- offer opportunities to coordinate PSMB investments with those in LMR networks or other state government programs (such as mobile black spots initiatives).

It is ultimately up to each jurisdiction to decide what level of statewide coordination to pursue.

Good procurement practices can deliver value for money

Good procurement is difficult. Governments do not have complete information about companies' cost structures, technical capabilities or intentions. Moreover, the challenges of designing a good tender process — and benefiting from competition between bidders — are amplified by Telstra's dominance in many areas (in mobile services and backhaul) and the relatively small number of equipment vendors.

However, state and territory governments are not powerless in dealing with mobile carriers and technology providers. They have several tools at their disposal to strengthen their bargaining position and/or facilitate competition in tender processes to deliver better value for money for taxpayers.

- Governments can split tenders (by technology or service, and/or on a regional basis) to allow more companies to participate, provided the competitive benefits outweigh the additional tendering and coordination costs. This approach has been used successfully in other government contracts, such as for rail infrastructure.
- Benchmarking bids against other cost data can help governments to assess bids that are submitted through a tender process. Transparency measures (such as 'open book accounting' provisions) might also provide a useful way to gauge the reasonableness of costs after a contract is signed.
- Negotiating collectively can exert countervailing power. One option for state and territory governments is to negotiate with potential suppliers on behalf of their PSAs to secure a better deal. State-owned infrastructure and spectrum holdings can also be used to reduce costs and give governments leverage in the negotiation process.

There are also strategies available to governments to reduce lock-in risks. For example, keeping customisation of equipment to a minimum, and insisting on the use of technology that complies with open international standards, can give governments the option to switch suppliers in the future. Moreover, aligning the length of contracts with the economic life of assets provides a way to avoid being locked in to a provider for longer than necessary. However, these are partial strategies, and it is unlikely that lock-in risks can be completely eliminated through contract design.

Finally, some participants have suggested that the PSMB procurement process should be designed with a view to promoting competition in the broader telecommunications market. PSMB procurement is unlikely to be the least-cost way of targeting competition objectives relative to alternative policy options (such as legislation governing competition and infrastructure access in telecommunications markets). Value for money should be the primary consideration for governments — attempting to target additional objectives through the PSMB procurement process could lead to unnecessary delays and costs.

Interoperability requires technical and institutional change

A nationally agreed set of technical standards — covering network and handset technologies, the ability of users to move between networks in different jurisdictions, and the compatibility of software — put in place by state and territory emergency services ministers, could facilitate technical interoperability between PSAs (within and across jurisdictions).

Ideally, standards should be put in place within one year. This would reduce the risk of 'early mover' jurisdictions locking in technologies that preclude future interoperability with other jurisdictions. A common standard need not preclude two or more jurisdictions working together to realise efficiencies (for example, by sharing parts of, or jointly procuring, a PSMB capability).

Institutional barriers to interoperability at the agency level, including an entrenched stubbornness to share information with other agencies, must also be overcome. Each agency will need to amend its processes and protocols for sharing and storing information, both with other agencies in the same jurisdiction and with their interstate counterparts. State and territory ministers can lead this process within their jurisdictions by setting clear expectations and deadlines.

Capacity sharing arrangements are efficient, but won't be easy

Many PSAs are used to having their own communications networks, or their own dedicated channels on a shared network (that is, a 'partitioned' network). However, this model would be an inefficient way to provide a PSMB capability, as it could constrain an agency's ability to scale up its data use during an emergency.

Sharing a PSMB capability requires PSAs within each jurisdiction to reach agreement on how users and applications are to be prioritised in specific operational situations. This will be challenging and contentious in some jurisdictions. There is a role for ministers to lead efforts to develop formal inter-agency protocols within their jurisdictions by setting clear expectations and deadlines for when these protocols need to be put in place.

Summing up

Taken as a whole, the Commission's analysis and findings represent a set of guiding principles to help governments in implementing a PSMB capability (box 6). Key features of an efficient implementation strategy are to promote efficient service provision, deliver the best value for money for the community, and be evidence based and accountable.

Box 6 Guiding principles for government action on PSMB

Promote efficient provision

- Price spectrum at its opportunity cost, regardless of how it is distributed or to whom.
- Ensure PSAs face the cost of delivering (and investing in) PSMB.

Deliver the best value for the community

- Base decisions about the capacity and quality of PSMB on the associated costs, benefits and risks — a uniform capability is unlikely to be efficient across jurisdictions.
- Rely on LTE technology and maximise the use of existing infrastructure, where it is technically and economically feasible to do so.
- Adopt procurement practices that facilitate competition in tender processes, strengthen the purchaser's bargaining position and reduce lock-in risks.
- Develop a common standard that supports technical interoperability across jurisdictions.
- Develop protocols and procedures at the agency level regarding the sharing of information and network capacity.

Be evidence based and accountable

- Undertake trials initially to build confidence in a commercial approach, to gauge the costs, benefits and risks of PSMB, and to gather evidence for a larger-scale rollout.

Draft recommendations, findings and information requests

Mobile broadband offers significant potential benefits

DRAFT FINDING 2.1

The land mobile radio networks used by PSAs are reliable and have extensive geographic coverage (voice only). However, they only support low-speed data applications, and they lack technical interoperability. This can prevent PSAs from communicating with one another, and means that radio equipment does not work upon crossing jurisdictional borders.

DRAFT FINDING 3.1

PSA use of mobile broadband applications has the potential to improve the quality of public safety services, the operational efficiency of PSAs and the safety of officers.

DRAFT FINDING 3.2

PSAs' uptake of mobile broadband applications is limited at present due to concerns about the quality of commercial mobile services. Critical issues include the ability of PSAs to get priority access to — and sufficient capacity on — commercial mobile networks during times of congestion, and the reliability of commercial networks relative to land mobile radio networks.

A PSMB capability must support mission critical situations

DRAFT FINDING 4.1

The communications needs of PSAs are characterised by high and non-predictable peak periods. PSAs can (and do) employ strategies to reduce their demands on communications networks during peak periods without any significant loss of benefits. Provisioning a PSMB network to meet relatively infrequent peak events would be prohibitively expensive.

DRAFT FINDING 4.3

PSAs expect a PSMB capability to deliver a standard of service that would allow them to use mobile broadband data applications in 'mission critical' situations (where there is a material risk of loss of life or severe injury).

However, operationalising the concept of a mission critical data network is difficult. The Commission has proposed a starting point definition for service quality. Specifically:

- the network should be available 99.9 per cent of the time, and cover at least 99 per cent of the population
- PSAs should be provided with priority access to (and capacity on) PSMB networks, with scope to change these arrangements in real time
- PSAs should be able to communicate with each other (within and across jurisdictions), including by accessing PSMB networks upon crossing jurisdictional borders
- communications over a PSMB network should be secure.

INFORMATION REQUEST

The Commission is seeking feedback on how it has operationalised the concept of a mission critical mobile broadband data network (draft finding 4.3).

DRAFT FINDING 4.2

PSAs' use of mobile broadband services and applications would likely increase significantly if a PSMB capability were available. However, the level of network capacity that PSAs would use is highly uncertain, as are the benefits of that use.

Options for delivering a PSMB capability

DRAFT FINDING 5.1

The costs of delivering PSMB under any option can be reduced by:

- maximising use of existing infrastructure
- sharing network capacity among PSAs in real time (that is, a non-partitioned network)
- allowing for flexible use of spectrum across users.

DRAFT FINDING 5.2

Providing a permanent PSMB capability in areas not currently covered by commercial mobile networks would be very costly. There are lower-cost options that can be pursued to provide a level of mobile broadband coverage and capacity (such as transportable equipment or satellite broadband), albeit not to a 'public safety' standard.

DRAFT FINDING 5.3

There are technical and institutional barriers to interoperability that will need to be overcome.

- Technical interoperability across mobile broadband networks requires compatibility of network equipment, end-user devices and software. A common and agreed set of technical standards can facilitate this.
- Agencies will need to develop protocols and procedures for storing and sharing information, both with other agencies in the same jurisdiction and with interstate counterparts.

DRAFT FINDING 5.4

It is technically feasible to deliver a PSMB capability under a dedicated, commercial or hybrid approach. However, the ability of commercial mobile carriers to provide PSAs with 'guaranteed' network access and priority over other traffic without dedicated spectrum is yet to be demonstrated.

INFORMATION REQUEST

To what extent do the current LTE standards support dynamic adjustment of the prioritisation of users or applications in real time? Can dynamic adjustment of prioritisation be on the basis of a user's role, agency or location? Using non-proprietary technology, is it possible for dynamic prioritisation to feature in commercial delivery approaches?

DRAFT FINDING 6.1

A commercial approach is the most cost-effective way of delivering a PSMB capability to PSAs. Preliminary analysis indicates that a dedicated network is nearly 3 times more expensive than a commercial option.

A hybrid option is also more expensive than a commercial option, though the cost difference narrows as the size of the dedicated network component of the hybrid option decreases.

DRAFT FINDING 6.2

There is risk and uncertainty associated with delivering a PSMB capability. Relevant risks include:

- technical risk (whether the capability meets PSA service requirements)
- commercial risk (supplier 'lock-in' and difficulties in contracting)
- third-party risk (potential impacts on non-PSA mobile users).

The nature and magnitude of risk varies across PSMB delivery options. For example, the risk of governments becoming locked in to using a single supplier is most pronounced under a commercial approach, while a dedicated network is most susceptible to delays and technological obsolescence.

Good implementation is essential to get the most out of PSMB

DRAFT RECOMMENDATION 7.5

If state and territory governments decide to deploy a PSMB capability, they should take a phased approach to implementation by first trialling a capability on a small scale. Trials would provide an opportunity to:

- demonstrate the technical feasibility of a commercial approach
- evaluate the costs, benefits and risks of PSMB
- develop protocols and procedures for information and capacity sharing by PSAs
- develop the business case for a wider-scale rollout.

Land mobile radio networks are expected to continue operating in all jurisdictions for at least five years, creating a relatively low-risk environment for experimentation with PSMB.

DRAFT FINDING 7.1

Prices that reflect the cost of providing a PSMB capability would encourage PSAs to use it efficiently.

DRAFT RECOMMENDATION 7.1

If state and territory governments decide to deploy a PSMB capability, police and emergency services ministers in each jurisdiction should set clear expectations and deadlines for PSAs to develop formal inter-agency protocols for:

- sharing information, including security procedures to safeguard sensitive information
- prioritising specific agencies, users, devices and applications, where a PSMB capability is shared among agencies
- specifying responsibility for administering these arrangements and exercising dynamic control over network settings.

DRAFT RECOMMENDATION 7.2

To facilitate an interoperable mobile broadband capability for PSAs, state and territory governments should task police and emergency services ministers with agreeing to a set of minimum common technical standards within one year. These standards should have the objective of facilitating national interoperability and should build on the *National Framework to Improve Government Radiocommunications Interoperability 2010–2020*.

DRAFT RECOMMENDATION 7.3

If the Australian Communications and Media Authority allocates spectrum for PSMB, it should be priced at its opportunity cost.

DRAFT FINDING 7.2

Using procurement processes for PSMB to target policy objectives other than value for money — such as promoting competition in parts of the broader mobile broadband market or meeting equity objectives — would be a blunt, costly and non-transparent way to meet those objectives. Other policy instruments are likely to provide more effective alternatives for achieving additional objectives.

DRAFT RECOMMENDATION 7.4

If state and territory governments decide to deploy a PSMB capability, they should maximise value for money in procurement by using competitive procurement processes. In doing so, they should adopt strategies to increase the number of potential bidders (such that all Australian commercial mobile carriers would be able to participate) and reduce the risk of becoming 'locked in' to a single supplier.

Strategies available to governments include:

- benchmarking bids against other cost data and making tender processes transparent
- splitting up tenders by service and/or region
- negotiating on behalf of their PSAs
- leveraging their infrastructure and spectrum holdings in negotiations
- using short-term contracts that require adherence to national technical standards and the ability of public safety officers to roam onto other networks.

Estimating PSMB costs

INFORMATION REQUEST

What types of costs arise from augmenting mobile carrier networks to meet PSA traffic? What is the appropriate approach to estimate these costs? Are there alternative methods that could be used as robustness checks?

INFORMATION REQUEST

What is the appropriate approach to estimate the cost of backhaul? How are backhaul networks designed to meet levels of traffic? How does this differ between PSMB delivery options?

1 Introduction

1.1 Background to the study

For emergency services, reliable communications can be the difference between life and death, both for their personnel and members of the public. At present, public safety agencies (PSAs) — the police, fire, ambulance and emergency services — primarily rely on narrowband radio networks that offer voice communications and some low-speed data services (including text messaging and database queries). These networks are built to a high standard and can be relied on in 'mission critical' situations.

PSAs are also making increased use of more advanced communications technologies. Some are using commercial mobile broadband services to send and receive images, text, video and voice messages. However, uptake of commercial mobile broadband services and applications by PSAs has been modest and limited to non-mission critical situations. This is because the services currently available on the commercial market do not meet the standards that PSAs require. It is unlikely that PSAs will fulfil their responsibilities efficiently if they continue to rely predominantly on narrowband technology.

Mobile broadband holds significant potential for PSAs and the communities they serve, in terms of cost savings and improved public safety outcomes (such as lives saved or injury and property damage avoided). The prospective benefits are manifold. Mobile broadband could allow police officers to collect and transmit key evidence when out in the field. Live video streaming between a fire crew and central command could improve situational awareness, ensure equipment and officers are deployed safely and efficiently, and expedite the evacuation of residents. And the ability for ambulance officers to remotely access medical records or send images to the hospital could speed up treatment and save lives.

Whether or not these benefits are realised largely depends on the availability of a 'public safety grade' mobile broadband capability that meets high standards for reliability, coverage and other characteristics. The consensus is that PSAs are unlikely to make significant investments in, or widespread use of, mobile broadband until such a public safety grade service is available. There is a risk that this will not happen within the next few years — or in a way that allows for interoperability across agencies and jurisdictions — without some kind of government intervention.

Delivering a mobile broadband capability that meets PSA requirements will be challenging. There are myriad possible approaches — including deploying a dedicated network, using commercial networks or some combination of these — and each leads to different technical challenges, costs and risks. Moreover, the benefits of each approach are highly uncertain, and contingent on operational and cultural change at the agency level to incorporate mobile broadband into activities and procedures and share information with other agencies.

A further complication is that no single model is likely to fit the different needs of each state or territory. Some jurisdictions already manage and invest in public safety communications on a statewide basis, and have recently upgraded their narrowband networks. Others have taken a more decentralised approach. The roles, responsibilities and operational requirements of individual PSAs differ across the country, and so one size will not fit all.

1.2 What has the Commission been asked to do?

The Commission has been asked to undertake a 'first principles' analysis of the most efficient, effective and economical way of delivering a public safety mobile broadband (PSMB) capability to PSAs by 2020. This is to include an assessment of the relative costs, benefits and risks of deploying a dedicated PSMB network, relying on commercial networks, and a combination of these.

The terms of reference set out several characteristics of a PSMB capability that the Commission must have regard to. These include the ability for the capability to be nationally interoperable, operate in both metropolitan and regional Australia, be resilient, and ensure accessibility, priority and sufficient capacity for PSAs. In addition, regard must be given to relevant domestic and international experiences, and work that has been undertaken to date.

The Commission has not been asked to evaluate whether a PSMB capability should exist at all. Rather, this study is about identifying how best to deliver a PSMB capability, giving consideration to the specific needs of PSAs, the relative merits of alternative deployment approaches, and the likely costs and benefits to the community. The impacts of alternative approaches are being weighed up to come to a view on the best way forward for delivering PSMB, including the appropriate roles for governments, PSAs and commercial carriers.

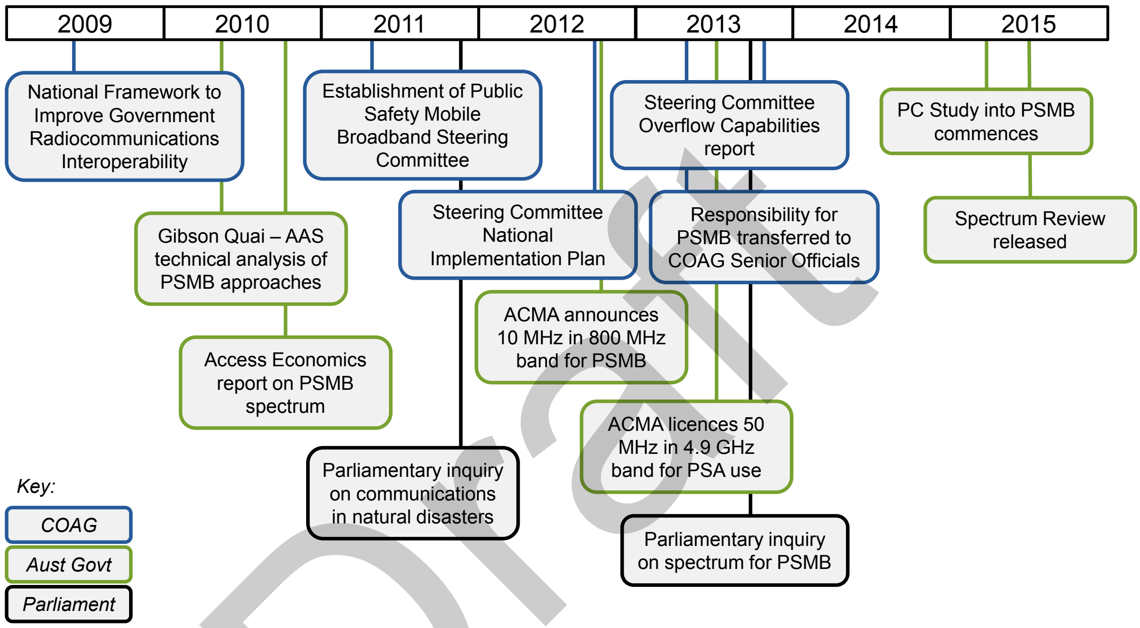
1.3 Domestic and international experiences

This study is being undertaken in the context of earlier work relating to PSMB, as well as parallel developments in Australia and overseas that are of relevance. Further detail is provided in appendix B.

Previous Australian reviews of PSMB

PSMB has been the subject of several reports and policy developments over the past five years (figure 1.1). This includes work by state and territory governments, as well as the Australian Government, under the auspices of the Council of Australian Governments (COAG).

Figure 1.1 **Previous developments relating to PSMB**



In particular, a detailed technical analysis was commissioned by the Australian Government in 2010 and released the following year. This work modelled the costs of delivering PSMB under several specific options, including a dedicated network, the use of commercially provided services, and various combinations of these (GQ-AAS 2010). It also involved building up a detailed picture of PSA requirements for mobile broadband, in consultation with PSAs across Australia. However, only limited parts of the report were made public.

In 2011, the Australian Government established a Public Safety Mobile Broadband Steering Committee, comprising senior officials representing government agencies, PSA peak bodies and the COAG Standing Council for Police and Emergency Management (Attorney-General's Department 2011). This committee was tasked with reporting on the most effective and efficient way to deliver a PSMB capability. It produced a detailed National Implementation Plan (in 2012) and an Overflow Capabilities report (in 2013), neither of which was released publicly. In April 2013, COAG transferred responsibility for PSMB to a group of senior officials (COAG 2013).

More broadly, jurisdictions have cooperated to improve the ability of public safety officers to 'interoperate' across narrowband communications networks. This culminated in the *National Framework to Improve Government Radiocommunications Interoperability 2010–2020*, which was endorsed by COAG in 2009 (COAG 2009).

Work on PSMB has also been undertaken in other forums. Much of this work has focused on the allocation of radiofrequency spectrum, since access to specific frequencies of spectrum is required to wirelessly transmit and receive information in any radio network. In particular, two parliamentary inquiries have investigated the communications (and spectrum) needs of PSAs (ECRC 2011; PJCLE 2013). Both recommended that the Australian Government allocate spectrum specifically for the purposes of constructing a PSMB capability.

Spectrum policy and licensing is the responsibility of the Australian Communications and Media Authority (ACMA). In October 2012, ACMA made an in-principle decision to set aside 10 megahertz (MHz) of spectrum within the 800 MHz band to support the deployment of a PSMB capability. It also announced that 50 MHz of spectrum in the 4.9 GHz band would be set aside for exclusive use by PSAs, and formally licensed this in June 2013. However, spectrum in the 800 MHz band is yet to be formally allocated for PSMB, and ACMA has indicated that it will take into account the Commission's study in reviewing the future use of this band (ACMA, sub. 14).

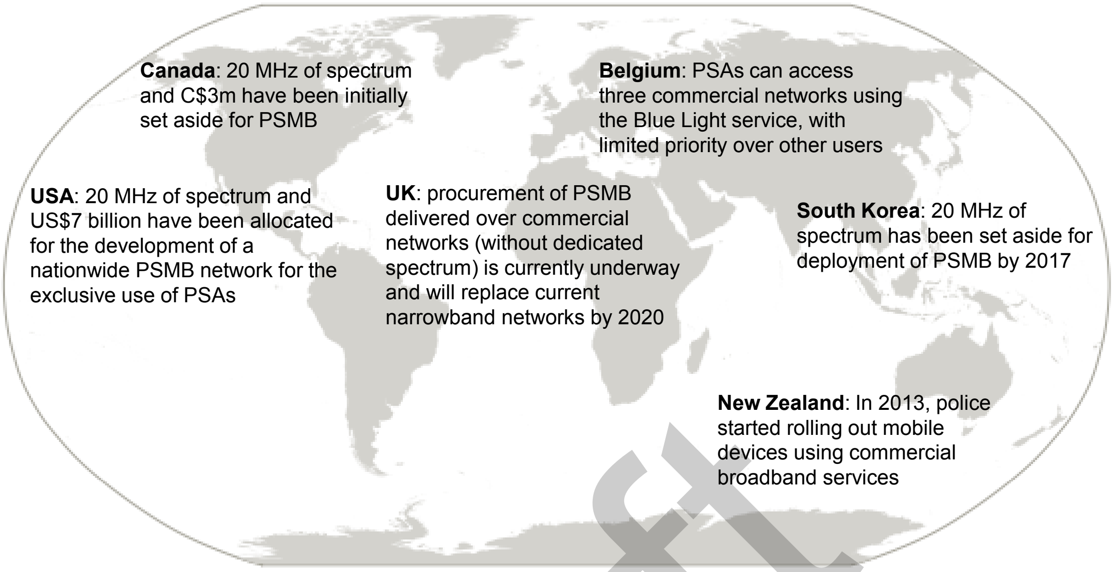
In addition, Australia's spectrum policy and management framework has been subject to a recent review (Department of Communications 2015b). Among other things, this review proposed replacing the current legislative framework with outcomes-focused legislation that facilitates more timely allocations of spectrum and greater flexibility of use, as well as allowing public sector bodies to lease, sell or share spectrum for their own benefit. The Australian Government recently announced that it would implement the main recommendations of this review from 2016 (Turnbull and Fletcher 2015).

Other countries are also pursuing PSMB

Several other countries are investigating, planning or implementing a PSMB capability. The specific approach taken differs across countries, with some closer to a dedicated approach and others more reliant on commercial networks (figure 1.2).

The United States, Canada and South Korea have all announced that they have set aside 20 MHz of spectrum in the 700 MHz band for public safety use, and all three intend to construct networks dedicated to delivering PSMB. By contrast, the United Kingdom and Belgium have sought to have mobile broadband delivered to their PSAs mainly over commercial networks, and under contracts that set specific service standards.

Figure 1.2 **International approaches**



Progress varies across countries. Only Belgium has a fully operational service, but it is not 'public safety grade' and mainly involves accessing a commercial service with limited priority given to PSAs over the networks. (New Zealand also has a commercial service, but this does not appear to involve any kind of preferential treatment for PSAs.) The United States, United Kingdom and South Korea are in advanced stages of planning for PSMB capabilities that meet high standards of reliability, priority and other requirements. By contrast, in Canada, many key decisions related to governance and service standards are yet to be made.

Alongside these developments, work has been underway in multilateral forums to harmonise technologies and spectrum use across countries. The 3rd Generation Partnership Project, which develops international technical standards for mobile broadband, has started to integrate specific public safety requirements into the standards. In addition, the International Telecommunications Union has suggested specific spectrum bands that can be used for public protection and disaster relief, including within the 800 MHz band in the Asia-Pacific region (encompassing Australia).

1.4 Stakeholder perspectives on PSMB

State and territory governments have primary responsibility for public safety, including by setting policy and funding PSAs. The Australian Government is also directly responsible for some PSAs, such as the Australian Federal Police. Governments are therefore ultimately accountable for the activities of PSAs and the outcomes they achieve for the community.

PSAs use a range of inputs to fulfil their duties, including communications technology. While there is nothing to prevent PSAs purchasing commercial mobile broadband services — and many are already doing so — governments may wish to intervene on behalf of their PSAs to secure a public safety grade service. This could be done to meet policy objectives that governments have set, including:

- national interoperability across agencies and jurisdictions
- delivery of PSMB by 2020
- broader public safety objectives.

Government involvement may also offer opportunities to achieve greater cooperation among PSAs and value for money in securing a suitable mobile broadband service.

PSAs' requirements are diverse

PSAs' communication needs have several aspects that distinguish them from the needs of other mobile broadband users. Communications tend to increase significantly during emergency incidents — which are often unpredictable — to many times the level during 'business as usual' periods. PSAs also need to rely on their communications systems in mission critical situations where lives and/or property are at risk, even where communications infrastructure has been damaged or mobile phone networks are congested.

These aspects have implications for the type of mobile broadband capability that PSAs require. PSA engagement in this study, as well as in past policy processes, has revealed several desired features of a PSMB capability. In broad terms, these can be categorised as quantity (the amount of data capacity on a network) and quality (the type of service).

Specific characteristics of a PSMB capability (reflected in the terms of reference) include:

- sufficient data capacity to support a range of applications, including text messaging, database access, location tracking and video streaming
- a wide coverage footprint, including in metropolitan and regional areas
- high levels of reliability, such that the network is always operational
- the ability to 'interoperate' across different agencies and jurisdictions

- the ability for public safety officers to establish a connection to their communications network and receive priority over non-PSA users, even during periods of congestion
- the ability to integrate voice communications
- a high degree of security.

There is broad agreement that a PSMB capability should be of sufficient standard to support the use of mobile data applications in mission critical situations. But there is less agreement on the specific service levels that would be required to meet this standard, and little work has been done to articulate these. In particular, estimates of the data capacity required to meet PSA needs vary considerably, with little consensus on the most appropriate level that should be delivered.

Individual states have progressed with PSMB

All jurisdictions have recognised the potential benefits of PSMB, and some have undertaken their own studies on how to deliver it (separate to activities conducted at the national level). In particular, both New South Wales and Victoria have investigated ways to establish a PSMB capability within their respective jurisdictions.

The NSW Telco Authority is currently undertaking an assessment of the costs and benefits of a PSMB capability in New South Wales (NSW Telco Authority, sub. 30). This has included a detailed assessment of the costs of specific delivery options, a bottom-up forecast of agency data requirements for mobile applications, and an evaluation of ways to maximise competition and efficiency in the delivery of PSMB. The work to date has not been made public.

The Victorian Government has commissioned studies on the benefits and costs of a national broadband capacity for emergency services (in 2011) and on international experience with public safety broadband (in 2013) (Victorian Government, sub. 28). Only the latter document has been made publicly available (Deloitte 2013).

Commercial solutions are starting to emerge

Technology companies, network operators and other private-sector entities have been active participants in policy processes relating to PSMB. Indeed, in Australia and other countries, commercial entities have begun to develop and trial mobile broadband solutions (including network equipment, handsets and service provision) targeted to meet public safety requirements. A prominent example of this is Telstra's LANES capability, a hybrid approach to PSMB that has been trialled in Queensland and Western Australia (box 1.1).

Box 1.1 **Telstra LANES**

Telstra LANES is a hybrid approach to public safety mobile broadband. It consists of a dedicated network using a dedicated spectrum channel that can only be accessed by users from public safety agencies (PSAs). When PSA data requirements exceed the capacity of this channel, users can seamlessly move onto Telstra's broader commercial network, where they receive guaranteed priority over other network users. This allows the network capacity available to PSAs to be scaled up instantly.

The capability involves integrating a dedicated channel of spectrum into a commercial carrier network and using a single core network to manage traffic from both public safety officers and non-PSA users. It is based on Long Term Evolution technology (also known as 4G) and draws on dynamic prioritisation techniques and public safety applications developed by Motorola Solutions.

Telstra LANES has been trialled in Queensland and Western Australia in 2013, and for the G20 Leaders' Summit in Brisbane in November 2014 (in both cases, using spectrum licensed to Telstra for the dedicated network component). Telstra has reported that these trials showed that PSAs could be given preferential data treatment over a shared network, and that users suffered no disruption of service while moving between the dedicated PSA capacity and the broader network capacity.

Source: Telstra (sub. 19; 2014a).

1.5 The Commission's approach

The Commission is focusing on the most efficient way for governments to implement a PSMB capability by 2020. Specifically, it is assessing the relative costs and benefits of a range of different approaches from the perspective of the community as a whole. This is guided by the *Productivity Commission Act 1998* (Cwlth), which requires that the Commission have regard to achieving higher living standards for all members of the Australian community.

The Commission has approached this task using cost–benefit analysis. This allows for a rigorous and consistent assessment of the costs and benefits (including those that are non-monetary) of a range of options for meeting a policy objective. This assessment is undertaken both quantitatively and qualitatively. Specifically, the Commission has:

- identified a range of 'scenarios' that describe the quantity and quality of mobile broadband services that a PSMB capability could deliver
- explored the technical and cost implications of using different inputs and deployment approaches to provide a PSMB capability
- evaluated the costs, benefits and risks associated with a set of specific delivery options
- quantitatively analysed the costs associated with each delivery option
- examined the institutional, governance and procurement aspects of implementing a PSMB capability.

In line with its standard practice, the Commission has sought to draw on publicly available information to the greatest extent possible. This is to provide transparency in the sources used to develop draft findings and recommendations, and to allow interested parties to replicate the quantitative component of the study. While some information was received on a commercial-in-confidence basis, it has not directly been included in this report. Where robust information or empirical data were not available to cite publicly, the Commission has made judgments. These are clearly indicated in the report. Feedback is sought on all assumptions and inputs that have been used.

1.6 Conduct of the study

The terms of reference for this study were received from the Treasurer on 25 March 2015.

To assist interested parties to prepare submissions to the study, the Commission released an issues paper on 20 April 2015. The Commission received 31 submissions in response to the issues paper from PSAs and their representative associations, Australian Government agencies, mobile network carriers and equipment providers. Four state and territory governments made a public submission.

The Commission met with a range of organisations, individuals, industry bodies and government agencies. Technical workshops were held in Melbourne and Sydney in June 2015 to discuss the approach to the quantitative component of this study. In addition, the Commission engaged the company UXC Consulting to provide technical input and expert advice on the quantitative analysis. Appendix A provides details of the individuals and organisations that have formally participated in the study to date.

This is a draft report. You are invited to examine and comment on it by written submission to the Productivity Commission **no later than 28 October 2015**. All submissions should preferably be provided as public documents that can be placed on the Commission's website for others to read and comment on. If, however, participants opt to provide material in confidence, it should be provided under a separate cover and clearly marked. Further information on how to provide a submission is included on the study website at www.pc.gov.au/inquiries/current/public-safety-mobile-broadband.

The Productivity Commission thanks all study participants for meeting with the Commissioner and staff, participating in technical workshops and making submissions to the study to date.

The final report will be prepared after submissions on the draft report have been received and stakeholder meetings have been held. It will be forwarded to the Australian Government by the end of December 2015 and released on the Commission's website a short time after.

1.7 Structure of the draft report

The remainder of this draft report is structured as follows.

- The next chapter reviews the current state of public safety communications and the associated shortcomings.
- Chapter 3 identifies the opportunities that mobile broadband offers PSAs and factors that may be limiting uptake to date.
- Chapter 4 assesses PSA requirements for mobile broadband and develops a set of scenarios to guide quantitative analysis of delivery options.
- Chapter 5 investigates the technical feasibility of, and cost drivers associated with, different approaches for deploying PSMB.
- Chapter 6 evaluates the costs, benefits and risks of a set of specific delivery options for PSMB, using both quantitative and qualitative analysis.
- Chapter 7 discusses the broader institutional, governance, regulatory and procurement aspects of implementing a PSMB capability.

Appendixes support the analysis in the main body of the draft report. Appendix A lists the individuals and organisations that have participated in the study to date. Appendix B reviews past work undertaken in Australia and relevant international experiences with delivering a PSMB capability. Appendix C provides the full technical details regarding the quantitative analysis undertaken by the Commission.

2 Public safety agency communications

Key points

- Historically, public safety agencies (PSAs) have communicated primarily using voice radio. However, some information that was previously communicated via voice is being digitised and carried over data services.
- PSA demand for communication services is not constant and varies in both a predictable (for example, on Friday/Saturday nights, and during major planned events) and unpredictable (for example, during emergencies) way, resulting in peaks and troughs in demand.
- The 'mission critical' nature of the work PSAs undertake distinguishes the communication requirements of PSAs from other users. While exact functional requirements will differ between PSAs, all agencies require their communication services to have high availability, security and reliability.
- Data capabilities are provided through both dedicated land mobile radio (LMR) data networks and through commercial 3G/4G mobile networks.
- LMR voice networks form the backbone of PSA mobile communications. These networks have extensive coverage and have proven to be reliable over decades of operation.
- Population coverage of LMR voice networks and commercial 3G/4G networks is similar across states and territories, although there are differences in geographic coverage.
- There are some issues with LMR voice networks:
  - the use of standalone networks based on different standards, frequencies and end-user devices has resulted in a lack of technical interoperability
  - there are examples of some LMR voice networks becoming congested, both during weekly peaks and during emergencies
  - several analogue LMR networks (mostly in regional areas) are yet to be encrypted, potentially compromising confidentiality and PSA operations.
- LMR data networks are typically more reliable than commercial mobile networks, but are limited in coverage (only available in some metropolitan regions) and can only carry low volumes of data. Commercial mobile networks have a much larger coverage area and achieve higher data throughput, but reliability concerns limit usage by PSAs to mostly non-mission critical situations.

2.1 Who are the public safety agencies?

Public safety agencies (PSAs) undertake a range of community safety and incident response activities, often in close collaboration with each other. The terms of reference state that PSAs include police, fire, ambulance and emergency services. For this study, emergency services include all agencies for whom emergency management is their core business, such as the State Emergency Service (SES), as well as marine search and rescue services provided by the Australian Maritime Safety Authority (SCRGSP 2015).

- *Police agencies* pursue the achievement of a safe and secure environment for the community, including through investigation of criminal offences, response to life threatening situations, and provision of road safety and traffic management. Police agencies also assist the judicial process by providing custody services.
- *Fire service organisations* work to minimise the impact of fires, which include structural fires, grassfires and bushfires, and vehicle and other mobile property fires. Fire services are also involved in search, rescue and recovery operations, fire prevention activities, and building community resilience.
- *Ambulance service organisations* prepare for, provide and enhance: pre-hospital and out-of-hospital patient care and transport; inter-hospital patient transport; specialised rescue services; ambulance services to multi-casualty events; and capacity building for emergencies.
- *SES* help communities prepare for, respond to, and recover from unexpected events, such as road accidents, floods, earthquakes, cyclones, and search and rescue.
- *Marine rescue and coast guard organisations* provide marine rescue, boating safety and communications services.

Other agencies such as Surf Life Saving Australia, Sheriffs' departments, Air Services Australia, and utility companies could arguably be considered in scope (CDMPS et al., sub. 7). However, while they all serve a public safety function or provide an important input to PSAs' activities, emergency management is not the core activity of these agencies. It is important to note that this will not preclude these agencies from accessing any future public safety mobile broadband (PSMB) capability. Indeed, any system developed to meet the requirements of the identified PSAs is likely to overlap with the requirements of other users.

As state and territory governments have primary responsibility for delivering emergency services, most PSAs are administered at the state or territory level. Generally, PSAs are run as public agencies by government department. A small number of PSAs are administered at the Commonwealth level, including the Australian Federal Police and Australian Maritime Safety Authority (SCRGSP 2015).

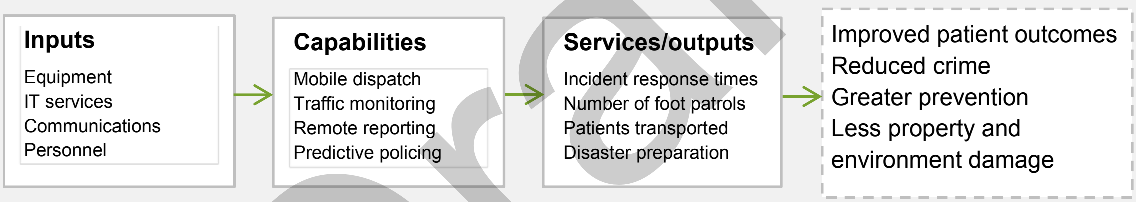
While there are commonalities between PSAs, no two agencies are the same. The scope of operational activities undertaken will vary with many factors, including the time of day, the day of the week (weekday or weekend), the time of year (summer or winter), and the area of operation (city, metropolitan or rural). While all PSAs require communication services to fulfil their responsibilities, with these differences in operations come different demands and requirements for communication services.

2.2 PSA demand for communication services

PSAs have a wide variety of resources at their disposal (box 2.1). For example, state-of-the-art helicopters capable of providing life-saving blood transfusions mid-flight, police scanners that automatically scan number plates to check vehicles against registration databases, and remote monitoring of a building's fire system.

Box 2.1 Value chain of PSA services

PSAs rely on multiple inputs to complete their missions, of which the ability to communicate is just one. Inputs include personnel (frontline officers, dispatchers, office staff, central command decision-makers), equipment (helicopters and vehicles to footwear and knee-pads), training, information technology systems and communication infrastructure.



Inputs equip PSAs with the capabilities necessary to deliver the services and outputs required of them. For example, the capability to dispatch jobs directly to emergency vehicles allows PSAs to provide timely assistance in life-threatening situations, and the ability to remotely lodge incident reports allows police officers to spend more time on patrol. Some of these outputs, such as incident response times, are measurable, although there are issues with the interpretation (for example, how response times impact on outcomes) and comparability (for example, differing calculation methodologies between jurisdictions) of such measures. Others are harder to quantify but nonetheless yield benefits for the community.

The work of PSAs is often time critical, and to effectively respond to an incident PSAs need information. The efficacy of PSAs is enhanced if they can deliver the right resources, at the right time, to the right location. An ability to automatically scan number plates is of little use if further information about the vehicle, persons and their history cannot be obtained.

Communication capabilities enable this exchange of information. These capabilities are not an end in themselves; rather, they form an essential input for PSAs to provide their services. The quality of communications affects PSA outcomes by increasing the efficiency of resource use, leading to either:

- a reduction in the cost of providing a given level of service
- an improvement in the service provided, for a given cost.

By reducing costs and enabling PSAs to provide more effective services, communities are the ultimate beneficiaries of PSA communication capabilities.

PSAs communicate using voice and data services

The information that PSAs send and receive comes in many forms including voice, text, image and video. Not all communication services can transmit these different forms of information equally (box 2.2). The communication services used to share and exchange this information fall into two broad categories: voice and data.

Box 2.2 The difference between communication services and applications

A communication *service* is a system of physical assets, operating software and technical standards that together provide a communication capability. For example, a 4G commercial mobile service is a combination of physical assets (such as transmission towers, backhaul links), operating software (core network architecture) and technical standards that in conjunction provide end users with the ability to communicate data.

An *application* is the means through which a service is put into use in pursuit of a certain function, task or activity. Applications can involve both software programs that run over a communication service and the peripheral devices that interface with the service. For example, Skype (an application) could use the National Broadband Network (a data service) to provide video conferencing (a function). Ambulance Victoria uses the Mobile Data Network (a service) to run Computer Aided Dispatch software and devices (an application) to assist them with rapid response to emergencies.

Generally, digital services permit a variety of applications, whereas due to technological limitations, analogue services permit only voice applications.

Voice services

Voice services allow real-time communication between PSA units, command centres and other resources. Historically, voice has comprised the bulk of PSA communications; if a PSA unit wished to determine the status of another unit, or to receive a dispatch from central command, voice communication has been the primary, if not only, means to communicate this information. Voice is still regarded as the paramount communications requirement for PSAs (P3 Communications and TCCA 2015).

Voice services are provided to PSAs using fixed, mobile and satellite technologies (section 2.5). Fixed-line voice services include all wired communication connections to a premise, such as copper and fibre networks. They typically provide better voice quality, reliability and security than mobile and satellite voice services, however with an obvious lack of mobility.

Many jurisdictions are in the process of upgrading their voice services from analogue to digital — in metropolitan areas in particular. This comes with significant benefits, including improved audio quality and the ability to integrate low-speed data services, enabling applications such as man-down alarms, Global Positioning System tracking, and encryption.

Data services

Information that is stored in digital form, such as text, images and video, can only be transmitted over a data service. This information is a series of on/off codes or 'ones and zeros' transmitted over either a wired network or the radiofrequency spectrum to a receiving terminal, which converts the signal back into a useful form (text, image, video or sound).

Data services have the advantage of being able to transmit information accurately, often without input or interaction by the receiving party and, with newer technology, can transmit a large quantum of information very quickly. Voice communications can also be digitised for transmission over a data network.

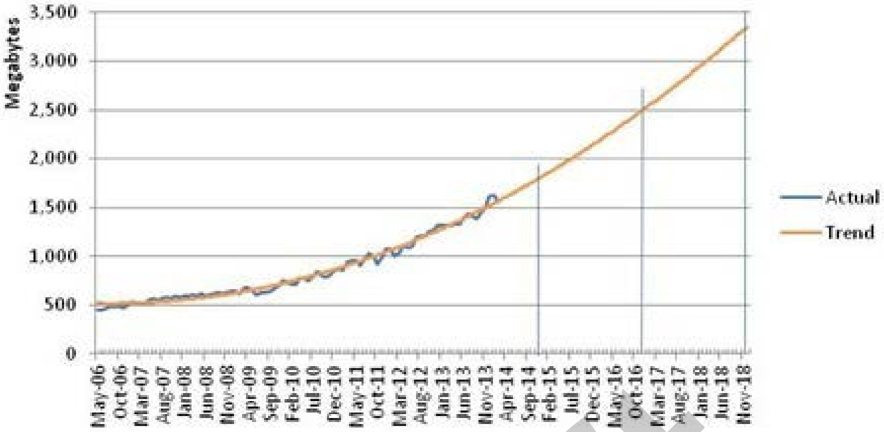
Increasingly, information that was communicated via voice is being digitised and carried over data services. For example, ambulance services previously used voice communications to dispatch paramedics and relay job information. This could include information such as incident priority, the best route to a given location, and special access information such as the location of house keys (Metropolitan Ambulance Service 2004). The advent of mobile data terminals means that this information can now be transmitted directly to the vehicle via text, helping ensure that human errors are minimised and freeing up paramedics' time for other uses.

Figure 2.1 shows how PSAs' use of the Mobile Data Network in Victoria has grown since 2006, with further growth projected in the coming years. PSA use of mobile broadband data services (currently and in the future) is discussed further in chapter 4.

To date, PSAs' use of mobile data services on their own land mobile radio (LMR) networks has typically been limited to these text-based applications. PSAs are starting to use mobile applications with higher bandwidth requirements, such as images and video. However, they are largely reliant on commercial mobile networks to provide these services.

Figure 2.1 **Mobile data use is increasing**

Mobile Data Network actual and projected usage, by month



Source: Weiss (2015).

2.3 How are PSAs communicating?

Both PSAs and the community hold information that is relevant for the provision of public safety and emergency services. PSAs generate, store and share a wealth of information, from personal information and criminal records stored in a police database, to the simulated movement of a fire front. Community members provide vital information to PSAs about the location and nature of emergency incidents, both when they occur and as they unfold.

Agency-to-agency communication

PSAs rely on communication systems for internal information sharing (with colleagues in the field or command) and to communicate with other PSAs and support agencies. The hierarchal structure of PSAs, with a chain-of-command and centralised decision making, results in a need for information to be ferried from frontline officers to their superiors and vice versa. This drives a two-way communication flow that is as demanding on sending information as it is on receiving, whether it be via voice or data. Depending on the information being sent, communication between public safety officers can be either one-to-one or one-to-many.

One-to-one communications

One-to-one communication refers to correspondence that is exclusively between two individual users on a network. PSAs use one-to-one communication both for voice and data. For example, officers responding to an incident will often have a need to communicate directly between one another within the incident site.

One-to-many communications

A key factor of PSA communications is heavy reliance on one-to-many communication, where many users can receive the voice or data transmitted by a single user. One-to-many communication is utilised when the information may be of value to multiple recipients, for example, weather forecasts and traffic updates. One-to-many communication also allows any user to monitor the actions and status of other users, so while the majority of people tuned-in to a given channel may not be the intended recipients of a message, all users can benefit via increased situational awareness (Minehane, Molloy and Burgan 2014).

Communication between the community and PSAs

An increasingly important aspect of PSA communication is the two-way flow of information between the community and PSAs. All PSAs have avenues through which the community can contact the agency to request assistance or to communicate information. These communications take the form of emergency calls for assistance (box 2.3), non-emergency calls for assistance (for example, patient transport requests), information on potential incidents (for example, reports of smoke or suspicious behaviour), requests for information (for example, burning-off procedures) and other routine calls.

Box 2.3 **Triple Zero services**

For emergency incidents, communication occurs primarily through the national Triple Zero service and the corresponding state-level emergency service organisation call centres. The Triple Zero service currently answers about nine million calls each year.

Mobile phones have become the primary device through which the Triple Zero service is accessed, with 67 per cent of calls placed by a mobile phone in 2012-13. This has created some problems for PSAs as, unlike landlines, the exact location of the caller is not provided automatically.

Triple Zero is a voice only service. However, it is envisioned that the Next-Gen Triple Zero service will incorporate greater functionality, such as text messaging, video capability and an enhanced ability to determine a caller’s location.

Source: Department of Communications (2014b).

Receiving accurate information from the community during an emergency is critical to PSAs achieving situational awareness. The higher quality the information PSAs receive about an event, the better placed they are to prioritise incidents and manage their assets.

Currently, PSAs rely heavily on voice communications for this information, sometimes leading to issues with accuracy.

Part of PSAs' mission is to provide timely and accurate information to the community so that it can prepare for or evacuate in the event of a disaster. Multiple avenues are used by PSAs to distribute information to communities, including:

- press releases and media events, which are carried by news organisations or published online
- warnings and emergency information broadcast on television and radio
- emergency details on PSAs' or other government websites
- Facebook, Twitter and other social media platforms
- community engagement for preparation and prevention activities.

In times of emergency the volume of these communications can be substantial. For example, during the four days of the 2013 Tasmanian bushfires, the Tasmanian Fire Service issued five bushfire advices, forty-six Watch and Act messages, thirty-nine bushfire emergency warnings, nineteen Emergency Alert messages (box 2.4); as well as advice through news outlets, ABC local radio, and online, and physical door-knocking (Department of Communications 2014b).

Box 2.4 **Emergency Alert**

Emergency Alert is the national telephone warning system used by emergency services to send voice messages to landline phones, and text messages to mobile phones located in declared warning areas. Negotiations, contracting and procurement for the system has been led by the Victorian Government on behalf of all states and territories.

To determine if a person is located in a warning area, Emergency Alert relies on the registered service address for fixed-line phones and the last known location and registered address of a mobile handset. For mobiles, this information is provided to Emergency Alert by the three mobile carriers, Telstra, Optus and Vodafone. Due to differences in how carriers collect these data, the ability for Emergency Alert to successfully determine a mobile handset's location varies between carriers.

Sources: Emergency Alert (nd); Victorian Government Solicitor's Office (2015).

2.4 Operational and functional requirements of PSAs' communication services

Communication services are critical to PSA operations

A key distinction between the communication needs of PSAs and those of the broader community is the mission critical nature of the work PSAs undertake. Because PSAs are often engaged in operations where the threat to lives or property is significant, they tend to have higher requirements for communication services with respect to availability, security and interoperability (chapter 4). Applications and communication services that meet these requirements are often described as mission critical, for example, push-to-talk voice, man-down alarms and Computer Aided Dispatch.

The nature of PSA work results in peaks and troughs in demand

PSA demand for communication services is not constant. It varies temporally and spatially. This is both predictable (Friday and Saturday night, major planned events) and unpredictable (emergencies). These periods can broadly be classified into four categories (Cornick and Gathercole 2012; VHA, sub. 11).

- Business as usual — such as undertaking activities that are everyday and routine, such as traffic management or transporting patients. During these periods, demand for communication services is expected to be relatively stable and predictable.
- Planned events — such as major sporting events, music festivals or G20 leaders' meetings which require a larger than usual PSA presence. During these events, demand for communication services is likely to be relatively high, but predictable.
- Localised, large-scale emergency incidents — such as fires in major buildings, bomb threats or other infrequent incidents which require a large and sustained cross-agency response. These events will likely entail high peak demand in localised areas. There is uncertainty about the timing and location of such incidents.
- Wide-area, large-scale emergency incidents — includes bushfires, major floods, cyclones and other emergency incidents that impact a wide geographic area. Typically, these occur in regional areas, although they can occur in major cities (for example, the 2003 Canberra bushfires). These incidents will likely entail high and sustained demand for communication services over a wide area. There is uncertainty about the timing and location of such incidents, although certain areas are historically more prone to such emergencies, which facilitates forward planning.

Each of these incident types places different demand requirements on communication systems.

PSAs have unique communication requirements

The operational and functional requirements PSAs seek from their communication services varies by agency, activity and location. For example, firefighting is conducted in harsh, physically demanding environments, and often across broad areas and remote locations. The needs of a firefighter and the demands she places on her communication system will differ from those of a police officer attending a localised emergency incident in an urban setting, or patrolling a music festival. For example, firefighters will typically require customised communication equipment to protect against risks of ignition and explosion that might otherwise be caused by the radio itself (MFB, sub. 6), a risk that is less pertinent to other PSAs. On the other hand, access to encrypted communication channels is of lower priority for firefighters than the police services, where unencrypted communications can have a severe impact on their operations.

Despite these differences, there are operational and functional characteristics of PSA communications that are shared across the PSAs. Examples of these are presented in box 2.5.

Firefighting communication requirements

Firefighters operate in physically demanding conditions that place extreme stresses upon both the communications equipment and the operator. Devices that are not shock, heat, and water resistant may fail in the harsh operating environment (SCF Associates 2014, MFB sub. 6). Firefighters wear bulky and often cumbersome safety equipment, such as thick gloves and breathing apparatuses, for which communication equipment must be compatible.

Voice communication is widely considered the most important and, in some cases the only, tool for coordinating resources at the fire front (SCF Associates 2014). Network coverage is a key consideration, with firefighters operating deep inside buildings, stairwells, basements, tunnels and remote bushland in regional areas. Hand-held radios must be high-powered to allow signals to be transmitted from these locations (MFB sub. 6).

It follows that voice clarity and speech intelligibility are key concerns for firefighters. Operation in noisy environments, compounded by the use, where necessary, of self-contained breathing apparatuses, can overwhelm a voice transmission to the point of inaudibility. Such situations require re-transmission, wasting valuable time, or may result in a complete breakdown of communication between firefighters and between firefighters and central control (SCF Associates 2014).

In regional areas, fire services rely heavily upon volunteer fire fighters. These volunteers are usually alerted to an emergency and the need to report to their stations via an emergency paging system. Accordingly, a reliable, wide-area paging system is essential to the operation of many fire brigades.

Box 2.5 Characteristics of public safety agency communications

High Availability — PSAs are unable to effectively provide their services in the absence of an ability to communicate. Networks should either have very high availability or have sufficient built-in redundancy options.

Extensive coverage — reflecting the geographic scope of PSAs, network coverage needs to be extensive. For some PSAs, this will include basements, stairwells, tunnels etc.

Relay capabilities — public safety officers need to maintain communication with the command centre and other units both from within their vehicles and when using handheld devices.

Voice

Voice clarity — voice communications must be clear and free from interference to ensure that information is relayed accurately and efficiently.

Push-to-talk — the ability, at the press of a button, to switch a communications device instantaneously from receive mode to transmit mode.

Dynamic talkgroups — the ability to group users onto their own virtual channel based upon a common communication need.

Direct mode operation — the ability for end-user devices to communicate directly with one another independently of the radio network.

Security and encryption — for safety and confidentiality purposes, PSA communications should be capable of only being heard by the intended recipient.

Data

Short data messaging and paging — send short messages to personnel without the need to use voice channels.

Computer Aided Dispatch (CAD) — used to dispatch resources to an incident, often in conjunction with a mobile data terminal. CAD applications have varying degrees of functionality ranging from simple job tasking and location tracking through to detailed incident information, routing, and status monitoring.

Automatic Vehicle Location — remote Global Positioning System tracking of vehicle location to aid in asset management and CAD.

Database access — mobile access to records, registries and other databases.

Man-down alarm — An alerting device that can be quickly and easily activated when the wearer is in distress and in need of urgent assistance.

Sources: CDMPS et al. (sub. 7); Minehane, Molloy and Burgan (2014); SCF Associates (2014).

Ambulance communication requirements

Ambulance services rely heavily upon data applications for communication, and are large users of commercial mobile networks. An entire job, including dispatch, patient information, mapping, vehicle location, and job status, can be handled without a single voice communication. (Queensland Ambulance Service, pers. comm., 26 August 2015).

This is not to say that voice is unimportant. Radio links to patient delivery destinations (such as hospitals) are still necessary for streamlining patient transfer (Queensland Ambulance Service, pers. comm., 26 August 2015). Medical emergencies that are specialised in nature or where the responding paramedic has limited experience may also require radio communication to off-site sources of medical expertise (SCF Associates 2014). Voice networks and procedures are also needed for redundancy, should there be issues with Computer Aided Dispatch or other data applications.

Ambulance services need communication security primarily for patient confidentiality purposes, since patient health information and medical records may be transmitted to responding units.

Police communication requirements

Compared to other PSAs, the police spend a greater proportion of time deployed in the field, typically on patrol or on duty in public places (SCF Associates 2014). Deployment in the field coupled with the mobile nature of police activities results in a large quantum of both voice and data communications. Among the PSAs, the police are the heaviest users of voice and data services.

Security of voice communications is of critical importance to police services. The nature of police work means that police officers are more likely to be the target of malicious actions by individuals or groups in the community than other PSAs. The ability for such people to intercept police communications, which may include details such as officer location, can put officers at risk. Further, police work can involve the need for secret tactical planning and the element of surprise, both of which are compromised when radio communications can be intercepted.

Police routinely query databases for information concerning persons or property of interest. Mobile access to these databases varies by jurisdiction but typically includes access to personal details, outstanding warrants, and vehicle and firearm registries. The frequency and importance of these queries to modern police work results in a strong reliance on data services.

2.5 Network infrastructure used to meet PSA communication needs

A combination of physical assets, operating software and technical standards is required to provide PSAs with a communication capability. This combination of inputs is generally arranged as a network, that is, a series of connections (whether wired or wireless) that allow two or more users to communicate data and/or voice.

To meet their communication needs, PSAs use a disparate set of networks owned by both commercial carriers and the PSAs themselves (box 2.6), including:

- land mobile radio
- commercial 3G/4G services
- fixed-line services
- satellite services.

Box 2.6 PSAs use both commercial and dedicated networks

Both commercial and dedicated networks are used to deliver communication services to PSAs. A dedicated network is a network that has been built for the exclusive use of PSAs (or a limited number of government agencies) and is specifically designed to meet PSA needs. In some cases these networks will be owned and operated by PSAs or the corresponding government agency. However, PSAs do not always own these networks themselves. For example, the Government Wireless Network in Queensland is owned, operated and managed by Telstra. The network has been designed specifically to meet the requirements of Queensland PSAs, and only the PSAs and select government agencies are permitted to use the network.

When using commercial services the PSAs are essentially like any other customer; they buy services on the open market that are provided on a 'best efforts' basis, that is, without any special arrangements concerning availability, priority or reliability. For this reason, commercial services are mostly used for operational and administrative purposes (chapters 3 and 4). Ongoing developments in the technical standards that underpin the delivery of mobile technology — and in particular 4G technology — is providing scope for PSAs to be offered better service levels using commercial networks (chapter 5).

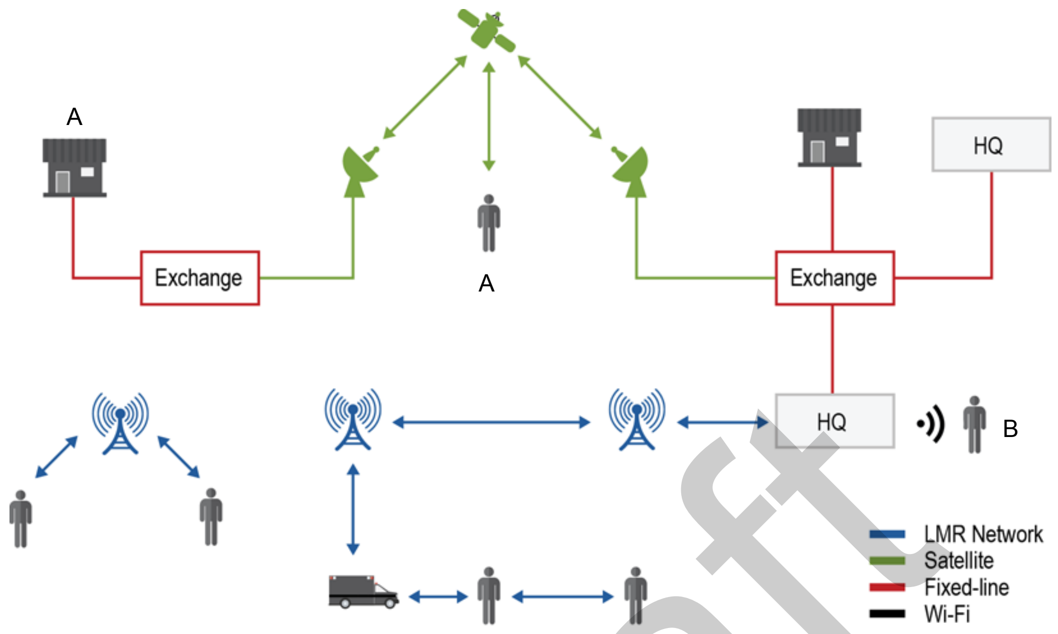
Key elements of communication networks

Although conceptually useful to think of communication networks as standalone, networks that are interlinked (through the use of 'gateway devices') can share common pieces of infrastructure (BAI, sub. 1). For example, in figure 2.2, when person A calls headquarters (HQ), both the satellite network and the fixed-line network are used to complete the call. Likewise, should person B wish to send an email to house A, the Wi-Fi, fixed-line, and satellite networks are used.

This 'any-to-any' connectivity is a standard feature of most communication networks, in particular those used by the public. For example, making a call between the Optus and Vodafone mobile networks is seamless. However, PSA networks are typically less interlinked than public networks due to differing (often proprietary) standards used on each network, because the gateway devices that link the networks are prohibitively expensive, or because the networks are truly standalone, that is, they are not physically connected to any other network.

Figure 2.2 **Communication networks**

Any-to-any connectivity of communication networks



Further, while commercial networks are often national or international in scope, dedicated PSA networks are typically delineated by jurisdictional boundaries. As responsibility for emergency management principally vests with state and territory governments, PSA networks are typically geographically dimensioned with only the state-level jurisdiction in mind. This has resulted in a clear demarcation of PSA networks at the jurisdictional boundary, which can lead to interoperability issues with cross-jurisdictional operations, particularly during large disasters (section 2.7).

Spectrum is an essential input into wireless networks

All radio networks, whether they carry voice or data, utilise the radiofrequency spectrum when transmitting signals. To minimise interference and to ensure spectrum is allocated to its highest value use, some parts of the radiofrequency spectrum are subject to detailed planning (box 2.7).

Wireless communication networks used by PSAs commonly use spectrum located in either the High Frequency (HF), Very High Frequency (VHF) or Ultra High Frequency (UHF) bands. As the choice of spectrum frequency comes with tradeoffs concerning coverage, building penetration, data-capacity and interference, the spectrum band deployed will in part depend on the performance requirements expected of the service (table 2.1). However, in general, long-range low data rate services such as paging are confined to frequencies in the VHF band (148–172 MHz); voice services are located in the lower parts (403–520 MHz and 820–870 MHz) of the UHF band; and services that require a very high data rate or for which a direct line of sight can be reliably established, such as network backhaul, Wi-Fi or satellite communication, are located in the upper portions of the UHF band.

Box 2.7 The need to plan spectrum

The range of available spectrum is theoretically infinite, however parts of the spectrum are more suited for a given use than others.

Lower-frequency signals are less affected by objects in their path, such as foliage and buildings, whereas high frequency signals can carry more data (where more bandwidth is available) but are limited to line-of-sight communication. This tradeoff leads to some parts of the spectrum being considered 'water-front property' for many uses, where an ability to propagate through built-up urban environments is balanced against the capacity to carry large amounts of information. Spectrum in this range (around 400 MHz to 900 MHz) is ideal for mobile telephony, television broadcasting and some types of radio communications.

It is not possible for everyone to transmit using the same frequency. In general, radio antennae cannot distinguish between multiple signals of similar strength on the same frequency, leading to interference between users. This rivalrous nature of spectrum necessitates regulation and planning of its use, which is achieved in three main ways:

- by restricting who can transmit on a given frequency
- by ensuring that there is sufficient separation between frequencies used to transmit a signal
- by specifying the maximum transmission power of devices and, hence, the geographical area in which that frequency is used.

In addition to preventing interference, planning allows countries to harmonise their use of spectrum. This involves designating certain frequency bands to be used for specific purposes, which allows both continuity of critical services between countries and the exploitation of economies of scale by industry. For example, the planning of transmission frequencies helps coordinate services that are international in nature, such as emergency and distress communication, maritime services, and aeronautical services. Businesses also benefit from technical standards that allow them to make devices that are compatible for use in multiple markets, leading to economies of scale.

Sources: ACMA (2013b); Carney, King and Maddock (2015).

PSAs use multiple standalone, single-application networks. The technical characteristics of spectrum combined with the limitations of analogue and early digital technologies have resulted in each application (or, where data services are concerned, a loose grouping of applications based on bandwidth) being provisioned over its own dedicated network. Further, lack of coordination between PSAs has in some areas led to a duplication of networks that both provide a similar capability but operate completely independently of each other. As a result, PSAs' communication needs are typically met through an abundance of standalone, single-application networks, often with each network operating on a different frequency and with different standards (figure 2.3). In some states (such as Victoria), these networks are shared between PSAs. However, in others, individual PSAs operate their own independent networks.

Table 2.1 **Propagation characteristics and uses of different frequencies used by PSAs**

Illustrative examples

	Frequency	*Propagation distance*[a]	*Foliage penetration*	*Typical use in radio communications*
High Frequency	3 to 30 MHz	50 to 1 000+ km	Highest	Long-range communication
Very High Frequency high-band	148 MHz to 172 MHz	5 to 120 km	High	Rural voice, paging services
Ultra High Frequency low-band	403 MHz to 520 MHz	1 km to 50 km	Low	Metropolitan voice and data
Ultra High Frequency mid-band	820 MHz to 870 MHz	0.5 to 25 km	Low	Dense urban voice and data
Ultra High Frequency high-band	Up to 2.5 GHz	line-of-sight	Lowest	Communications backhaul, Wi-Fi, satellite

[a] Propagation distance is also a function of output power. Values are for typical power outputs.

Sources: ACMA (2009); Victorian Department of Justice (2010).

The first four applications of figure 2.3 (analogue and digital voice, paging, and narrowband applications) are supported by different types of dedicated LMR networks. With the recent development of commercial mobile broadband services (circa mid-2000s) and the wide availability of broadband internet, broadband applications such as imaging and video are available to PSAs in some areas.

Land mobile radio networks

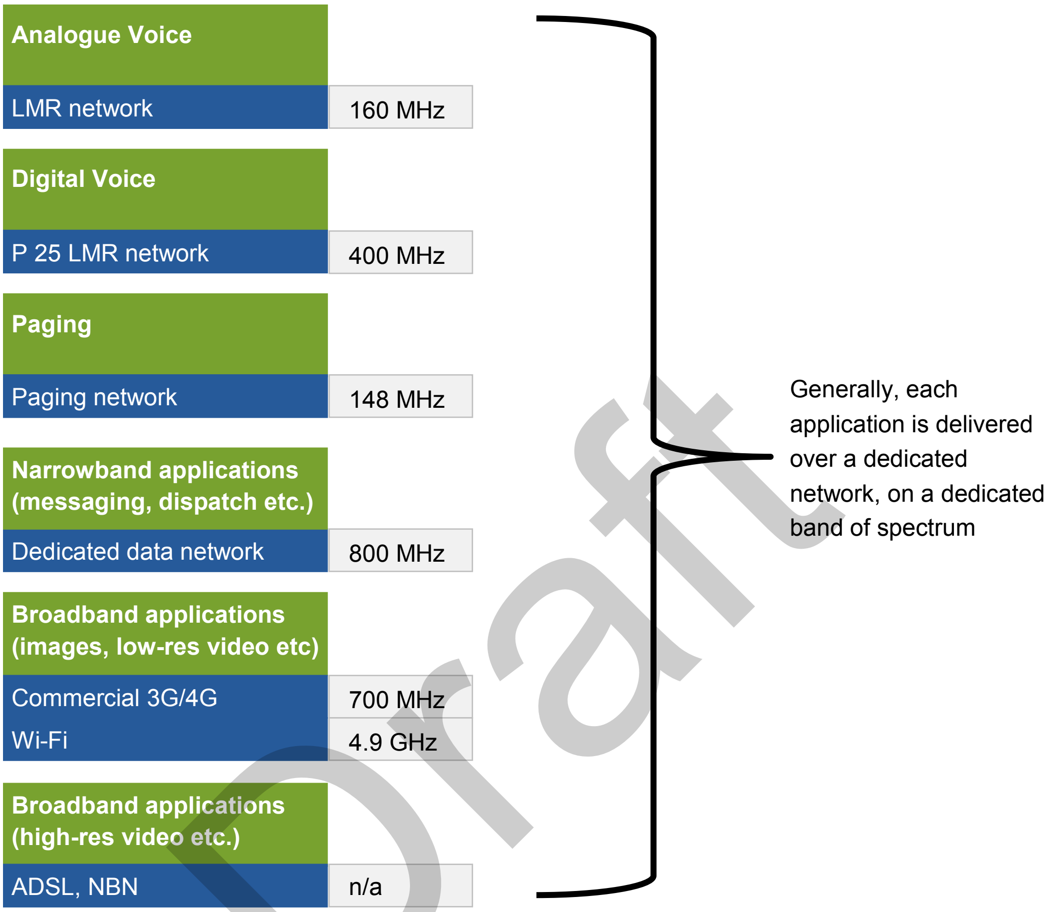
LMR networks enable wireless communication between land stations (typically towers, but may include aircraft or maritime stations), mobile stations and end-user devices such as handsets and Mobile Data Terminals (ACMA 2014e).

LMR networks can be grouped into three types, based on the applications that the networks support:

- voice networks (colloquially known as ‘two-way radio’ networks), which can be either:
  - analogue — capable of transmitting analogue voice. These networks have extremely limited data capabilities.
  - digital — capable of transmitting both digital voice and low-speed data.
- dedicated data networks — networks used exclusively for data transfer. These may have been considered high speed upon deployment, but are generally seen as low-speed by today’s standards.
- paging networks — simple alerting and text messaging.

Figure 2.3 **A disparate set of networks is used to deliver a suite of applications**

Based on Victorian PSA communication infrastructure



Sources: ACMA (2012a); Victorian Department of Justice (2010).

Different types of LMR networks can be both complementary or substitutable for each other. For example, data networks are complementary to voice networks: they introduce new capabilities to PSAs, such as the ability to access databases, but cannot completely replicate the push-to-talk functionality of a voice network. This is also true of paging systems, as the ability to send out an alert to personnel is an integral, but distinct, part of PSA communications. Accordingly, in a given jurisdiction these networks are typically run in parallel with one another.

Analogue and digital voice networks are substitutable, but in practice PSAs often continue to run analogue networks where digital voice is available. This is a byproduct of the piecemeal approach to upgrading analogue voice networks to digital, where only parts of a network are upgraded at one time.

LMR voice networks

LMR voice networks form the backbone of PSA mobile communications. Trunked analogue networks (box 2.8) constitute the largest radio communication networks used by PSAs across Australia, although digital networks are used in all capital cities.

Box 2.8 Trunked radio and Talkgroups

Radio communications occur over ‘channels’ — a slice of spectrum centred on a given frequency. In analogue networks each channel can only carry one voice transmission at a given time; if someone else is transmitting on that channel, then no one else will be able to transmit until the channel is clear.

One way to organise networks is to group users by either functional need or geographic location and assign them a specific frequency to use for radio communications. This approach raises two issues:

- there are only so many channels available, limiting the number of ‘groupings’ that can be made
- these channels will often be left idle, representing an inefficient use of resources.

Trunked radio is a computer controlled system that allows sharing of radio channels. Instead of reserving a physical channel for exclusive use by one user group, users are grouped into virtual channels called ‘talkgroups’. When a member of a talkgroup wishes to communicate, the computer finds an unused channel and automatically moves all members of the talkgroup to the new channel. Unless the network is congested, this all occurs automatically and in a fraction of a second, such that the switch in channels is unnoticeable to the user.

Trunked radio systems either enable communication to take place with fewer designated channels or, for a given number of radio channels, a greater number of user groupings. Either way, the end result is a more efficient use of spectrum resources.

Source: RadioReference (2015).

Analogue LMR networks possess many of the operational and functional requirements sought by PSAs, including:

- push-to-talk
- direct mode operation
- the ability to set up talkgroups
- high availability
- relay capabilities
- one-to-many communications.

Digital LMR networks meet the same operational and functional requirements of the analogue networks, but with the addition of clearer voice, greater capacity, and additional functionally, such as man-down alarms, GPS tracking and encryption (box 2.9).

Box 2.9 Examples of applications available over data networks

The applications available to PSAs over their data networks vary between jurisdictions. The following examples are illustrative of major metropolitan regions around Australia.

Victoria Police

- Computer Aided Dispatch link to the Emergency Services Telecommunications Authority
- Access to the Law Enforcement Assistance Program, a fully relational database that stores details of all crimes brought to the notice of police as well as family incidents and missing persons.
- Access to firearms and vehicle registries
- Shift reporting and remote submission of patrol duty running sheets
- Support for BlueNet Automatic Number Plate Recognition program

Victoria Ambulance

- Computer Aided Dispatch link to the Emergency Services Telecommunications Authority
- Event information, remarks and real-time updates
- Relay resource status and availability back to dispatch
- Ability to log and submit employee information

Sources: Victoria Police (2015); Victorian Auditor-General (2014); Victorian Department of Justice (2010).

LMR paging networks

All states have a dedicated LMR network for paging purposes. Paging is used primarily as an alert tool, notifying personnel of a need to either contact an operator for further information or to report to their stations, where further information will be provided. Paging networks are a one-way broadcast, with generally no means for the recipient of the message to use the network to communicate back to the controller. As the data requirements of a page are low, often consisting of only a few lines of text, and coverage is of paramount importance, paging networks typically operate at lower frequencies.

Paging networks are known to suffer from reliability issues, especially throughout periods of congestion. During emergencies it is not uncommon for messages to be significantly delayed or fail to be delivered to their recipients. For example, during the 2009 Victorian bushfires, the transmission speed of the paging system was reduced to expand reception coverage, leading to serious delays in all but the most urgent messaging (VBRC 2010). Compounding the issue is an inability for PSAs to see if their message has been delivered, with the corresponding uncertainty as to whether alternative communication channels should be mobilised. In some cases PSAs are using text messages as a form of redundancy to the paging network.

LMR data networks

For the purposes of this study, the term 'LMR data network' will be limited to standalone networks deployed for the specific purpose of supporting applications that rely on data. Under this definition, digital LMR voice networks would not be considered data networks. While the digital LMR voice networks currently used in Australia all have some ability to send data, the networks are generally very slow (for example, P25 phase 2 networks — a commonly used standard — achieve maximum speeds around 20 per cent of a dial-up modem) and the vast majority of their capacity is used for voice communications.

Information sent over a LMR data network is typically displayed to the user via a Mobile Data Terminal (MDT). These are in-vehicle computerised devices consisting of a screen, keypad, periphery devices and associated software. The applications available to PSAs will depend on the technical specifications of both their MDTs and the LMR data network, as well as the software and database architecture of PSAs' information technology systems. Applications that run on hand-held devices, such as iPads, are typically provided over commercial networks, not LMR data networks.

Commercial mobile voice and 3G/4G networks

PSAs use commercial mobile networks for voice and data communication both officially, that is, through contracts and arrangements with the commercial carriers, and unofficially at the initiative of individual members (including volunteers).

Commercial mobile networks are used extensively to meet PSAs' back-office and administrative communication needs, including voice services for non-frontline staff and management, remote access to email, and general mobile web-browsing. The relatively non time-critical nature of these applications means that occasional service unavailability, while undesired, can be tolerated. More recently, some PSAs have begun utilising commercial mobile networks to assist with everyday activities and provision of services (box 2.10).

Commercial services are being used 'unofficially' by public safety officers

It is difficult to determine the extent to which public safety officers use their own devices on commercial mobile networks while at work. However, anecdotal evidence suggests this use is not insignificant. Use appears to be more common in volunteer organisations such as the SES and volunteer fire brigades, often for coordination purposes. For example, upon receiving a paging message, SES volunteers may liaise outside of official channels to coordinate their response (although this is not endorsed or encouraged by organisational practice or policy) (Victorian SES, pers. comm., 6 August 2015).

PSAs operating in rural areas have also been known to use commercial mobile networks and Citizen Band radio when encountering blackspots in LMR voice network coverage

(Victorian SES, pers. comm., 6 August 2015). However, while unofficial use of personal devices on commercial networks may have tacit approval in some circumstances, the Commission has heard that some PSAs have banned these devices outright out of safety and confidentiality concerns.

Box 2.10 Applications used over commercial broadband services

Many PSAs are starting to integrate mobile devices running over commercial networks into their operations (chapter 3).

- Most states' police forces are in the process of distributing tablets and other mobile devices to their members. For example:
  - as of April 2015, the Queensland Police Service (QPS) had distributed 2000 iPads to field officers. Amongst other functions the QLiTE application, built by QPS' internal information technology team, enables remote access to state and federal databases, and supports a streamlined infringement issuing process.
  - in early 2015, NSW police commenced a trial of 500 Samsung tablets, allowing police to access databases, issue infringements and record intelligence while on patrol.
  - the Northern Territory Police Force is undertaking a similar iPad roll-out to all of its 1300 frontline officers.
- The Queensland Ambulance Service is rolling out an iPad application that allows paramedics to report patient cases while on the road. Paramedics can now receive the details of a job directly from central dispatch and enter patient information into the system while on the move.
- South Australian Ambulance Service vehicles have been fitted with mobile data terminals. Since late 2012, paramedics responding to an emergency are given on-the-road updates about the patient and the incident via a real-time feed from the ambulance dispatcher in Adelaide.

Sources: Cowan (2014); Coyne (2015); Moran (2013); Francis (2015).

Fixed line networks

PSAs use fixed-line networks to obtain broadband internet, voice telephony, teleconferencing, video conferencing, and fax services. These services are almost wholly supplied by the commercial sector. Fixed line services are also used to support other communication services, such as Triple Zero calls (box 2.3) and the Emergency Alert system (box 2.4).

Wi-Fi networks

Wi-Fi is a wireless network technology standard. The term Wi-Fi has become synonymous with enabling devices to access a fixed-line home or office broadband connection through a wireless access point. Wi-Fi uses spectrum located in the internationally recognised

2.4 GHz and 5 GHz bands, but power restrictions typically limit public Wi-Fi equipment to ranges measured in the tens of metres (ACMA 2014g).

As Wi-Fi is essentially an extension of a fixed-line broadband connection, the technology supports all data applications that can be used over the internet and 3G/4G networks. Wi-Fi is ideally suited for short-range, high capacity networks either temporarily deployed in support of an incident (such as mesh networks), or permanently fixed in areas with high expected use or throughput requirements (such as video surveillance links, or in command centres) (ACMA, sub. 14). PSAs are yet to fully integrate deployable Wi-Fi networks into their regular operations, so on a practical level the use of Wi-Fi is currently restricted to either office and business applications or non-real-time applications, such as ‘store-and-forward’ or ‘data off-load’, where information is stored on a device until it comes within range of an appropriate connection.

Satellite networks

Satellite is used primarily for communication in areas of Australia where there is no LMR or commercial network coverage. This includes large parts of Western Australia, Queensland, South Australia, the Northern Territory, western New South Wales and mountainous regions of Victoria and Tasmania. Satellite also acts as a redundancy measure should primary communication networks fail.

Although satellite networks possesses a vast coverage footprint, the technology is no panacea. Satellite communication can be impacted by weather events such as storms, heavy rain or smoke and ash clouds, limiting availability. This is problematic for PSAs as many of their peak communication needs occur during events characterised by these weather phenomena. Further, satellite coverage is not universal, with regions of reduced reception or complete black spots.

Capacity of data networks

All networks have a different capacity to carry data. The speeds achieved by the user depend on many factors, such as the number of people accessing the network, the location of the user (near the tower or at the cell edge, proximity to an exchange), or whether they are inside or outdoors (chapter 5), making precise comparisons difficult. However, as each network typically represents a several-fold or even an order of magnitude difference on other technologies, precision is not needed to compare the capabilities of different networks. Table 2.2 compares the range of typical speeds a user could expect on networks employed by PSAs.

Table 2.2 **Speed and coverage comparison of data networks**
Differences in data rates and coverage of common technologies

Technology	*Typical data rate (approximate)*	*Current coverage area*
Fixed-line broadband	50 000 kbps	na
Wi-Fi coupled with fibre connection	50 000 kbps	30m (indoors, public license)
Wi-Fi coupled with ADSL 2+ connection	10 000 kbps	30m (indoors, public license)
4G	14 000 kbps	Approx. 3% of landmass[a]
3G	3 500 kbps	30% of landmass
Satellite	2 600 kbps	Fixed-line footprint
LMR data network [b]	96 kbps (max data rate)	Most capital cities
P25 digital network	9.6 kbps (max data rate)	Metropolitan and some regional areas

[a] Based on 94% population coverage (Telstra, sub. 19) and an assumption that these networks cover the most densely population regions. [b] Based upon Victoria's Mobile Data Network. **na** Not available.

Sources: iiNet (2015); Motorola Solutions (2011); NBNCo (2014); OpenSignal (2015); Simpson (2014); *Sydney Morning Herald* (2014).

Coverage footprints of voice and data networks

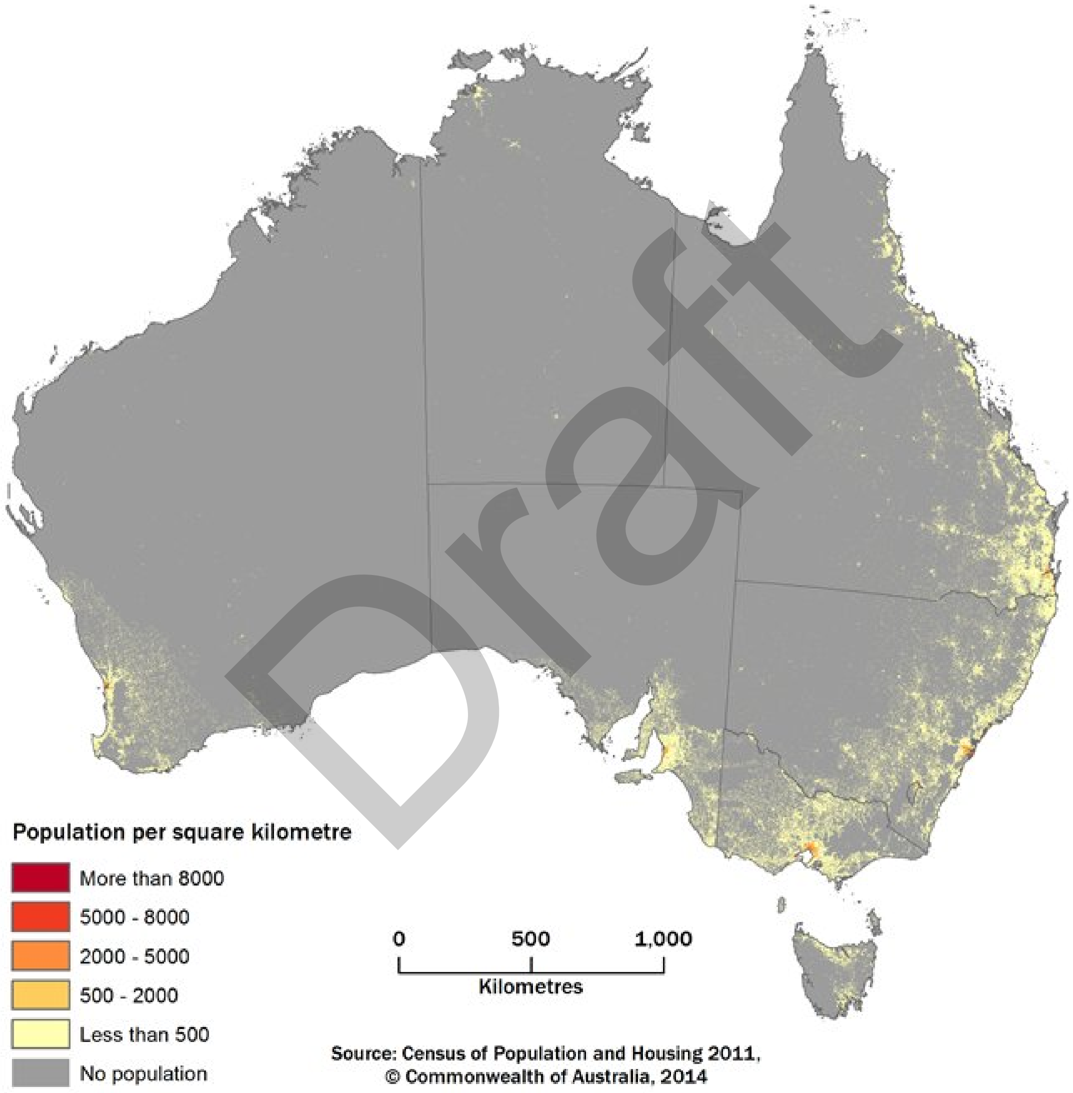
To perform their duties effectively, PSAs require access to a suite of communications tools which work irrespective of geographic location or population density. Depending on the incident, PSAs might need to operate in remote areas, deep inside buildings, or below ground.

Two metrics are used to measure the coverage of communication networks: geographical coverage, that is, the proportion of the total landmass covered; and population coverage, that is, the proportion of population covered by the network based on residential address. Geographical coverage is important to PSAs as, for some, their operational jurisdiction extends statewide, with an obligation to respond to an emergency regardless of location. However, as the majority of PSAs' activities are undertaken within or close to the community, coverage must include as large a proportion of the population as reasonably possible.

All states achieve high population coverage, but geographic coverage varies

The topography and population distribution of Australia means that the population coverage of communication networks is much higher than geographical coverage. Most of Australia's population is concentrated in the south-eastern and eastern coastal regions, and the south-west corner of Western Australia (figure 2.4). Within these regions the population is further concentrated in urban centres, particularly the capital cities. This means that it is possible to dimension a network to cover only a relatively small proportion of a state's landmass yet still cover a large majority of its population. In this way, geographical coverage of the different communication networks (paging, LMR and commercial 3G/4G) varies greatly between states, but population coverage of these networks remains close to uniform.

Figure 2.4 **Australian population density, 2011**



Source: ABS (2014).

Some PSA networks — such as StateNet in Victoria and the Tasmanian Ambulance Service LMR network — provide extensive geographic coverage of their jurisdictions, at around 95 per cent (Victorian Department of Justice 2010). Geographic coverage in other states is lower, reflecting either their topography or population distribution. The combined coverage of the LMR networks used by PSAs is difficult to ascertain as networks often overlap, methodologies for calculating coverage can be different (for example, in-car or handheld), or the combined coverage area is unclear due to differences in how jurisdictions report coverage levels. Anecdotal evidence suggests that combined LMR voice networks have a larger geographic footprint than any other communication network operating in Australia, except satellite. However, this may overstate the coverage available to any one PSA, as rarely do PSAs have end-user devices that can access networks in other jurisdictions or even equipment to access the networks of other PSAs in their state or territory.

PSAs also supplement their permanent LMR networks with temporary transportable coverage. Transportables can be used in two ways:

- to provide greater *coverage* in areas where there is currently no or very poor reception
- to provide greater *capacity* in areas where there is coverage but when it is overwhelmed during an incident.

In many jurisdictions individual PSAs have deployed their own standalone LMR voice networks. Often this has been for security reasons, such as a need to limit the audience of police communications, but it is also a byproduct of communication responsibility historically falling within the remit of individual PSAs rather than a coordinating state-level body. This is the case in:

- Tasmania, where Tasmania Police operate a separate network to the joint Tasmanian Fire Service and Ambulance Tasmania networks (Tasmanian Auditor-General 2014)
- Queensland, where in some regional areas the Queensland Police Service, Queensland Fire and Rescue Service and Queensland Ambulance Service all operate on separate networks
- Western Australia, where St Johns Ambulance operates a dedicated statewide system.

These networks are dimensioned in a way that reflects the needs and operational reach of each agency, which may be overlapping but will not be identical (MFB sub. 6).

Coverage of LMR data networks is limited to metropolitan areas

Some Australian capital cities (such as Perth, Sydney and Melbourne) have deployed a LMR data network.

Increasingly, coverage footprints of LMR data networks are being augmented with coverage from commercial mobile networks. This is enabling PSAs in some regional areas to access data-based applications, while also providing a redundancy measure for blackspots and outages experienced within the original LMR data network. For example, the second generation of Mobile Data Terminals used by Victoria Police was installed to allow roaming onto Optus' 2G/3G commercial network outside the coverage of the Mobile Data Network. A third generation of terminals currently being trialled will enable roaming onto Telstra's 3G /4G network on a 'best efforts' basis, effectively achieving whole-of-state population coverage.

2.6 Institutions, governance and regulatory arrangements

Primary responsibility for emergency management rests with state and territory governments — they have discretion to set their own emergency management agenda along with the accompanying appropriation decisions, including how much funding will be available and how it will be distributed between agencies. The Australian Government's role is largely limited to leadership on issues that require coordination, such as spectrum allocation, and supporting states and territories to develop their capacity for dealing with emergencies and disasters. This may involve physical and financial assistance to states or territories when they cannot reasonably cope during an emergency (PC 2014a).

Arrangements in states and territories

Emergency services constitute a ministerial portfolio in all states and territories, with the minister holding wide ranging responsibilities relating to appropriation, policy development and crisis management. Precise administrative arrangements differ between the states and territories, although generally the various fire and SES agencies are administered together, with police administered separately (in most cases under the same minister). Ambulance services are also administered separately, either under the department of health or fully privatised.

All jurisdictions procure communications services independently of each other. In some states (for example, Victoria, New South Wales and Queensland), major procurements of communications services are handled through a central agency. The role of these agencies is to provide a centralised resource for coordination and expertise, which allows PSAs and other government departments to focus on their core missions, and to realise scale efficiencies (NSW Telco Authority 2015; PSBA 2015). In cases where a central communications agency does not exist, PSAs are responsible for procuring their own communications services.

For commercial services, individual PSAs are responsible for their own procurement and contracts.

Coordination across jurisdictions is improving

To date, national emergency planning across the states and territories has been piecemeal and lacked national coordination. Following the 2009 Victorian bushfires and other natural disasters in the mid-to-late 2000s, governments at all levels recognised the need for a more cooperative and collaborative approach (COAG 2015).

At the intergovernmental level, the Council of Australian Governments (COAG) is the principal forum through which state cooperation is advanced. In 2009, COAG tasked the

National Emergency Management Committee to drive and coordinate the development of the National Strategy for Disaster Resilience, a whole-of-nation approach to disaster management (Australian Emergency Management Institute 2011). Through the Standing Council on Police and Emergency Management, COAG continues to work on improving disaster relief and recovery arrangements, including the *National Framework to Improve Government Radiocommunications Interoperability 2010–2020* (box 2.11).

Box 2.11 National Framework to Improve Government Radiocommunications Interoperability

In 2009, the Council of Australian Governments endorsed the *National Framework to Improve Government Radiocommunications Interoperability 2010–2020*, developed in collaboration with the National Coordinating Committee for Government Radiocommunications.

Noting that agencies responding to emergencies are often hampered by low levels of radio communication interoperability, the National Framework provides guiding principles and key areas of work for jurisdictions to enable transition towards interoperability. The Framework aims for all Australian governments to transition their domestic radio communications equipment to interoperable systems, modes and frequencies by 2020. A mid-term review is scheduled for mid-2015.

Source: COAG (2009).

States and territories are at different stages of the LMR network procurement cycle

Each state and territory government makes investments into LMR infrastructure based on its own budgetary priorities and PSA requirements. As a result, not all jurisdictions are at the same stage in the procurement cycle (table 2.3).

Table 2.3 Recent procurements

	Cost	*Install date*	*Expected life*
Melbourne Metropolitan Radio Network	$261 million	2004	9 years
South Australian Government Radio Network	$175 million (upgrade)	2017	12 years
Government Wireless Network (Qld)	$457 million	2014	15 years
NSW Government Radio Network (NSW)	$250 – $450 million	1993	Rolling upgrades
NT Digital radio	$13 million	2010	na
Mobile Data Network (Vic)	$140 million	2006	9 years
Police Metro Radio Network (Perth)	$58 million	2007	na

Sources: CDMPS et al. (sub. 7); Critical Comms (2015); NSW Telco Authority (2015); The Drum (2010); VDTF (2015a, 2015b). **na** Not available.

Some states, such as Queensland and South Australia, have made significant recent investments into digital radio for their PSAs. These investments are expected to have a life of between 12 and 15 years, with contracts for service extended as far as 2029. Other jurisdictions have either made these upgrades earlier (such as Victoria) with the assets currently 'midlife', or are expected to upgrade their digital radio networks in the near future.

Arrangements at the Australian Government level

The Australian Government acts as the coordinating body for issues of national interest. This includes administration and funding of the Australian Federal Police and Australian Maritime Safety Authority, spectrum planning, and broader legislative and enforcement responsibility relating to competition and infrastructure access.

The Australian Government has responsibility for spectrum planning

As a rivalrous, non-excludable resource, spectrum requires management and coordination to maximise the value of its use. In Australia, spectrum is managed by the Australian Communications and Media Authority (ACMA), an independent statutory authority whose objectives, responsibilities and powers in relation to spectrum management are detailed in the *Radiocommunications Act 1992* (Cwlth) and other related legislation (box 2.12).

Box 2.12 The Australian Communications and Media Authority

The Australian Communications and Media Authority (ACMA) is the independent statutory authority responsible for regulation of most elements of Australia's media and communications landscape. Through regulations, derived standards and codes of practice, ACMA seeks to ensure that Australia's media and communications sectors operate effectively and efficiently, and in the public interest.

ACMA is a 'converged' regulator, created to bring together the regulation of the main channels of communications: telecommunications, broadcasting, radio communications and the internet. ACMA has responsibilities under four principal acts: the *Radiocommunications Act 1992* (Cwlth), the *Telecommunications Act 1997* (Cwlth), the *Telecommunications (Consumer Protection and Service Standards) Act 1999* (Cwlth) and the *Broadcasting Services Act 1992* (Cwlth). ACMA also has responsibilities under other Acts, such as maintenance and monitoring of the Do Not Call Register.

ACMA manages spectrum in accordance with the Radiocommunications Act. This Act gives ACMA powers related to the planning of radiofrequency spectrum for specific uses, the licensing of radiocommunication spectrum and equipment, and powers to issue standards and other technical regulations.

Source: ACMA (2014d).

Spectrum planning is carried out in concordance with an overarching international framework. Under the auspices of the United Nations, the International Telecommunication Union (ITU) issues the *Radio Regulations*, a supranational technical document that allows for coordination on radio communication issues such as spectrum allocation and harmonisation. As a signatory to the ITU, Australia has obligations under international law regarding compliance with these regulations (appendix B).

In carrying out its duties, ACMA prepares a spectrum plan which divides available spectrum into frequency bands. The *Australian Radiofrequency Band Plan* is the broad level technical map that allocates certain sections of the radiofrequency spectrum to various types of services. The Band Plan is modelled upon and kept in line with the ITU *Radio Regulations* (ACMA 2013b).

For some of these bands, in particular those which are congested, ACMA will prepare a more detailed frequency band plan. These plans are used to provide a more detailed description of spectrum allocation applicable to different services, often down to individual channel assignment. The spectrum bands that PSAs use to operate their radio communication equipment are mostly subject to detailed frequency band plans.

PSA radio communications are migrating to the 400 MHz band

In 2008, ACMA conducted an extensive examination of PSA communication needs through a wide-ranging review of the 400 MHz band. As part of a holistic strategy to meet PSAs' voice, data and video communication needs, ACMA decided to migrate all government radio communications to the 400 MHz band (ACMA 2012a). Several segments of this band have been identified for the exclusive use of government, primarily to support national security, law enforcement and emergency services.

Harmonising government services into a single band is a necessary step to achieving national interoperability between PSAs and other emergency services agencies (ACMA 2014a). ACMA commenced this migration in 2012, with key milestones set for government agencies to transition to the harmonised band (ACMA 2015b).

- 31 December 2015 — relocation of government services in high- and medium-density areas into the harmonised government band.
- 31 December 2018 — relocation of government services in low-density and remote areas into the harmonised government band.

As of June 2015, 54.5 per cent of total apparatus licences in these bands had transitioned ahead of the milestone (ACMA 2015c).

2.7 Limitations of current PSA communication capabilities

The communication capabilities of PSAs are different from state to state, and PSA to PSA. Considering there are eight states and territories in Australia and three major PSAs in each state or territory, it is not practical for the Commission to assess the suitability of current arrangements for all 24 individual cases. However, there are some common themes.

LMR voice networks are resilient and have extensive coverage

The LMR networks used by PSAs have proven to be reliable in a range of strenuous circumstances, over several decades of operation. While not infallible, LMR networks are often the only communications network that continues to operate during disasters, such as the 2011 Queensland floods and 2015 Hunter Valley floods. New digital LMR networks are being built to a ‘five nines’ (99.999 per cent) service standard, or the equivalent of a maximum of 5.26 minutes of down time per year.

The geographic coverage of LMR networks is extensive. In most states, no other network offers the same geographic coverage of the combined LMR voice networks, although there are some caveats. LMR networks are adept at covering large areas and penetrating foliage, but lack in-building coverage in some areas. Blackspots are also present, most often in remote regions (VBRC 2010).

LMR voice networks lack interoperability

The use of standalone LMR voice networks based on different standards, frequencies and using different end-user devices results in a lack of technical interoperability, that is, an inability for one set of equipment to communicate with another set on a technical level. This results in several issues for PSAs.

- PSA radio equipment may not work in other states. This is a particular problem when PSAs are deployed interstate during large-scale emergencies.
- PSAs within the same state using separate networks will not be able to communicate directly with each other without expensive network bridging equipment.
- PSAs will be limited to the coverage footprint of a single network.

Some PSAs have arrangements in place to work around interoperability issues. For example, Victorian Country Fire Authority radios are installed in all Melbourne Fire Brigade appliances, and the Department of Environment and Primary Industries maintains a cache of radios to provide to other agencies (VBRC 2010). However, these arrangements are expensive and are not scalable in a way that provides universal technical interoperability.

In jurisdictions where technical interoperability is possible, procedural and operational barriers to interoperability remain. All PSAs use a command hierarchy to some extent, whether to ensure proper accounting and efficient use of resources or as a means by which superiors can maintain situational awareness. Such a structure cools enthusiasm for allowing public safety officers to communicate directly with one another. Terminology can also vary between agencies. Chapter 7 discusses steps governments and PSAs can take to improve operational interoperability.

LMR voice capacity is insufficient in some areas

LMR networks are at different stages of their asset lifecycles. For some, this means that dimensioned capacity is in excess of what PSAs currently use. For example, the Government Wireless Network in Brisbane had ample spare capacity during the G20 Leaders' Summit, which is likely to be the largest operation that the area will see for the operational life of the network.

There are examples of LMR networks becoming congested, both during weekly peaks and during emergencies. Congestion has proven to be a problem during emergencies (such as the 2009 Victorian bushfires and the 2011 Queensland floods), particularly in rural and remote areas. Some networks (such as the Metropolitan Mobile Radio network in Melbourne) suffer from congestion each evening as additional protective service officers start their shifts (Victorian Auditor-General 2014).

Analogue LMR networks lack security

Historically, voice transmitted over an analogue LMR network has been unencrypted. This exposes PSA communications to interception by members of the public who own the appropriate equipment, such as police scanners. More recently, radio communications have been available for streaming from dedicated websites or via mobile phone apps.

Upgrades to digital radio systems in many states and territories have improved the security and integrity of these systems. However, several analogue LMR networks (mostly in regional areas) are yet to be encrypted, meaning that anybody with an internet connection can listen in to these radio communications, potentially compromising confidentiality and PSA operations.

LMR data networks are slow and have limited coverage

The dedicated LMR data networks deployed in some metropolitan areas are slow when compared to commercial offerings (section 2.5). This limits the type of applications that can be used over the network to those with very low throughput requirements (such as text-based queries and photos). Coverage of these networks is typically limited to metropolitan regions, with extensions throughout the state (where offered) via roaming agreements with commercial mobile carriers. These roaming agreements are on a 'best efforts' basis and do not guarantee PSAs the same level of service as on the dedicated LMR data networks.

Commercial networks are used to support operational activities but do not meet mission critical standards

Commercial mobile broadband services provided on a 'best efforts' basis have proven to be highly beneficial in supporting police operational activities, but cannot be relied upon for mission critical applications. In particular, PSAs have suggested that there have been instances where the coverage and capacity of the commercial networks has not met users' expectations (MFB, sub. 6; Victoria Police, sub. 17).

At present, the reliability of commercial networks does not match that of LMR voice networks. While rare, events do occur in which commercial networks are unavailable for an extended period of time, such as during the 2015 Hunter Valley floods or the 2014 Warrnambool exchange fire. In both these incidents LMR networks continued to operate despite one or more of the commercial networks being unavailable.

DRAFT FINDING 2.1

The land mobile radio networks used by PSAs are reliable and have extensive geographic coverage (voice only). However, they only support low-speed data applications, and they lack technical interoperability. This can prevent PSAs from communicating with one another, and means that radio equipment does not work upon crossing jurisdictional borders.

3 Framework for analysis

Key points

- Public safety agency (PSA) use of mobile broadband applications has the potential to improve the quality of public safety services, the operational efficiency of PSAs and the safety of officers.
- Take up of mobile broadband applications by PSAs has been limited due to concerns about the quality of commercial mobile broadband services. Key issues include the ability of PSAs to get priority access to — and sufficient capacity on — commercial mobile networks during times of congestion, and the reliability of commercial networks relative to land mobile radio networks.
- The Commission has undertaken a first principles analysis to determine the best way to deliver a public safety mobile broadband (PSMB) capability by 2020. The analysis has involved:
  - understanding the mobile broadband requirements of PSAs, in terms of network capacity and quality of service
  - identifying options that could feasibly meet these requirements, including a dedicated PSMB network, an approach reliant on commercial networks, and a hybrid approach
  - evaluating the costs, benefits and risks of each option from the perspective of the community as a whole.
- Data limitations and uncertainties mean that not all costs, benefits or risks can be quantified. In particular, a lack of suitable information has meant that the benefits and risks of each option cannot be quantified in monetary terms.
  - As the options under evaluation have been designed to deliver a similar level of PSMB capability, the impact of each option on public safety outcomes (and thus, its benefits) is not expected to vary markedly.
- The Commission has also examined broader considerations that will need to guide policy decisions, including governance models, procurement processes and the practicality of implementation.

This chapter explores the opportunities that mobile broadband offers public safety agencies (PSAs) and the factors that may be limiting uptake to date. It also describes the Commission's first principles approach to analysing the best way to deliver a mobile broadband capability to PSAs.

3.1 Mobile broadband can enhance public safety

Mobile broadband (and the applications it supports) is dramatically changing the way people communicate and share information. However, PSAs' uptake of mobile broadband has been modest to date due to concerns about the quality of service offered over commercial mobile networks and the inability of land mobile radio (LMR) networks to support data-rich applications. Greater use of mobile broadband could be achieved (and the associated benefits realised) if PSAs had access to a capability that is better aligned with their needs.

Mobile broadband is changing the way people share information

Mobile broadband refers to the wireless delivery of an internet service over a mobile network, including through phones, tablets and portable modems. The underlying technologies used to deliver mobile broadband have undergone significant advances — from the 2G networks that have transferred voice calls and text messages since the 1990s, to the 4G networks that allow real-time video streaming today (box 3.1).

Box 3.1 Evolution of mobile broadband

Several technologies have been used to provide mobile data services in Australia. The three major commercial carriers (Telstra, Optus and Vodafone) operate several overlapping networks, using different technologies, and most user handsets can access more than one type of mobile network.

- 2G (GSM) networks were launched in Australia in 1993. These provide digital voice communications as well as low-speed data, including text messages, multimedia messages and caller identification.
- 3G and 3G+ (WCDMA and HSDPA) networks were introduced in Australia in 2005 and deliver significantly faster data rates than 2G networks. Services on these networks have enabled mobile internet browsing, and audio and video streaming.
- 4G (LTE) networks were launched in Australia in 2011. These enable even faster data speeds, with lower latency (delays) and reduced network congestion. 4G networks can provide peak download speeds of up to 100 megabits per second, rivalling the speeds offered by some fixed-line networks.

Ongoing investment in 3G and 4G networks means that 2G networks may be shut down in the near future. For example, Telstra has announced that it will close its 2G network by the end of 2016.

At present, the three commercial carriers are continuing to expand their 4G networks to meet a similar level of population coverage as their 3G networks. Data transfer happens over both the 4G and 3G networks (depending on a user's handset and location, and congestion on the network). At present, voice calls and text messages are only transferred over 3G and 2G networks. However, Telstra and Vodafone have announced plans to begin providing voice services over 4G networks during 2015.

Sources: ACCC (2015b); ACMA (2014c); Kidman (2015); Telco Antennas (2014).

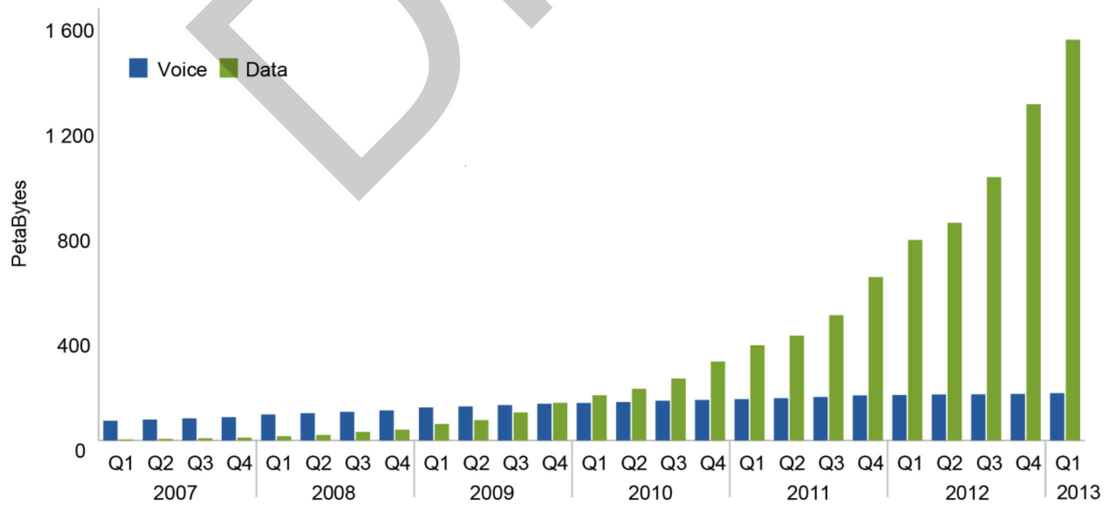
Mobile broadband technologies are still evolving: new features are being added to 4G networks (and the underlying technical standards) each year (chapter 5). Some companies have even started referring to, and sought to develop, 5G — the next generation of high-speed mobile broadband technology (Analysys Mason 2015).

The use of mobile broadband by consumers and businesses has grown rapidly (figure 3.1).

- The number of mobile broadband subscriptions globally has increased twelve-fold since 2007, and these now outnumber fixed-line internet connections (ITU 2015).
- In Australia, total mobile broadband data use increased tenfold in the three years to 2014 (ACCC 2015b), and has been projected to increase by 38 per cent each year between 2013 and 2017, with traffic over 4G networks in particular increasing at 76 per cent annually (CIE 2014).
- As of 2014, over 12 million Australians used a smartphone (ACMA 2014c).

Mobile broadband has had a substantial impact on the Australian economy. For example, a recent survey of businesses attributed an average saving of 1.4 per cent in overall operating costs to mobile broadband (CIE 2014). It can also increase business productivity by facilitating more productive use of time (allowing internet access from anywhere) and faster decision making. Businesses use mobile broadband in a range of ways, including through corporate applications and online data storage, and to engage with customers.

Figure 3.1 **Global data traffic in mobile networks**



Source: Ericsson (2013a).

Mobile broadband presents a significant opportunity for public safety

Public safety operations are becoming increasingly information driven. Mobile broadband applications (such as location tracking, biometrics, live video streaming, image transfer and dispatch messaging) offer significant potential to improve the efficiency and effectiveness of public safety services, fundamentally changing the way these services are delivered.

For example, mobile broadband applications can allow:

- police officers to access databases when out in the field, to use facial recognition technology or electronic fingerprint matching (biometrics) and to collect and transmit key evidence
- ambulance officers to remotely access medical records and expert assistance, or send images to the hospital while in transit
- fire officers to remotely access maps, building plans and locations of hazardous materials to locate incidents more quickly and identify how best to respond.

The community is the ultimate beneficiary of these applications, through reduced property damage and crime, fewer injuries and deaths, and better quality health care.

Mobile broadband also provides a way to more effectively share information between the community and PSAs. Members of the public are increasingly providing agencies with valuable information — such as photos of unfolding crimes and live video of floods and bushfires. The potential benefits of this information was widely recognised by study participants (for example, ATF, sub. 4; MFB, sub. 6; Victoria Police, sub. 17). However, the ability to share this data with officers in the field is limited at present (chapter 2).

PSAs are already using some mobile broadband applications (over commercial mobile networks) to establish and maintain a common operational picture between field officers and command, and between individual officers (box 3.2). PSAs are predominantly relying on commercial mobile services to support these applications. These are provided on a 'best efforts' basis — that is, PSAs are treated more or less equally with other customers over the commercial networks.

DRAFT FINDING 3.1

PSA use of mobile broadband applications has the potential to improve the quality of public safety services, the operational efficiency of PSAs and the safety of officers.

Box 3.2 How are PSAs using mobile broadband applications?

Ambulance

The NSW Ambulance Service currently uses mobile broadband to check and update electronic patient records in transit, reducing the time spent on administrative tasks and enhancing the quality of services delivered to patients. There has also been some use of high-bandwidth video to provide early remote diagnosis and treatment of stroke victims. The NSW Telco Authority has identified this as an important source of benefits from PSMB.

Fire and rescue

NSW Fire and Rescue is using mobile broadband for:

- Automatic Vehicle Location services, which can facilitate faster vehicle dispatch
- a first responder in-vehicle tablet application that provides officers with information and remote access to operating guidelines and databases
- in-vehicle applications for voice and video communications and inventory checks.

In Victoria, the Metropolitan Fire Brigade uses unmanned aerial vehicles to capture photos and videos of areas that are difficult or dangerous to reach, thus saving time, protecting officers and enhancing situational awareness.

Police

In 2013, Victoria Police started using an application to simplify processes for family violence reporting. It allows officers to pre-populate reporting forms with information already captured and stored in databases. As information is entered into the application it is instantaneously updated in the database entry. Reporting changes are estimated to have released an extra 72 000 police hours for patrol and proactive duties, at an equivalent value of $3.8 million.

Victoria Police also uses commercial mobile broadband in its ‘BlueNet’ traffic enforcement vehicles, which are equipped with in-car video, automated number plate recognition systems (to alert officers of stolen vehicles, unregistered vehicles, or other offences linked to a number plate) and mobile terminals that provide remote database access.

Tasmania Police recently replaced 1100 desktop computers with tablet devices, providing officers with remote access to secure databases and other applications. Officers can now write up statements from witnesses and victims of crime, as well as accident and crime reports, in the field, resulting in more time spent out in the community. Time savings over the six-week trial were estimated at one day per tablet used.

The Commission understands that police in other Australian jurisdictions are also using mobile broadband for database checks, administrative tasks and other purposes.

The New Zealand Police force began a roll-out of smart phone and tablet devices in 2013, with 7000 iPhones and 4100 iPads issued to frontline officers. Significant benefits were achieved, including an estimated time saving of 30 minutes per officer per shift, mostly due to mobile broadband applications that allow officers to respond to situations more effectively and move from one job to the next without returning to the station.

Sources: Acer Computer (2014); MFB (2013); New Zealand Police (2014); NSW Telco Authority (sub. 30); R Host (Fire & Rescue NSW, pers. comm., 14 July 2015); Telstra (2015b); Victorian Government (sub. 28); Victoria Police (2014).

There is a widely held view among study participants that PSA use of mobile broadband has been modest and piecemeal to date, and they are not fully realising the opportunities that mobile broadband presents. Participants suggested various ways that PSAs (and the broader community) could benefit from using mobile broadband more expansively (box 3.3).

The main reason for low uptake of mobile broadband is the lack of a guaranteed quality of service offered over commercial mobile networks. Study participants pointed to the fact that PSAs are not offered priority access on commercial networks during times of network congestion. They also expressed concern about the coverage of commercial networks (relative to LMR networks), and the susceptibility of commercial networks to outages during natural disasters and other kinds of interruption (MFB, sub. 6; PFA, sub. 8).

Box 3.3 PSAs could make greater use of mobile broadband applications: participant views

Study participants strongly supported providing PSAs with a public safety grade mobile broadband capability.

> [I]t is our firm view that police and ambulance officers, firefighters, paramedics, and other public safety agency frontline personnel have demonstrated a clear need for a dedicated nationwide wireless broadband network to support their operational needs. (BAI, sub. 1, p. ii)

> [H]aving 21st Century mobile broadband communications is also vital to police officer work health and safety, particularly officers working on the front-line. Police officers need the best in intelligence about offenders they are pursuing, up-to-date situational awareness, and data, video and other forms of critical information to operate most effectively and safely in the interests of the community and their own welfare. (PFA, sub. 8, p. 2)

> Reliable broadband data capabilities will support the exchange of timely and accurate information in the field. Integrating agency networks enables better coordination and improved service delivery outcomes for the community. (Victorian Government, sub. 28, p. 6)

Video based applications are seen as offering significant benefits to PSAs. These applications can improve the situational awareness and preparedness of PSA officers, and facilitate the provision of remote medical support.

> Sharing live video feed among PSA officers in the field and backend command control centre is becoming very important for these entire PSMB operational scenarios. (NEC, sub. 5, p. 5)

Participants also considered that a PSMB capability could be used to enhance PSA communication with the public.

> With regard to communications between the PSA's and the community, it is critical in times of disaster, both for the PSA's to advise community safety aspects, but even more importantly as part of the information gathering systems as in many cases it is data on 'social media' that provides an additional information to incident commanders on how to respond. (ATF, sub. 4, p. 11)

> Communications between PSAs and the community is a growing area of focus within Victoria. Traditional means of communications, such as radio and television are now augmented by a range of new media including mobile apps, social media, web pages, Emergency Alert, Next Generation Triple Zero etc. Broadband communications infrastructure to reliably inform the community of vital emergency information is already regarded as a mandatory requirement … (Victorian Government, sub. 28, p. 15)

As a result, PSAs tend to limit their use of mobile broadband applications to low-risk situations, and are reluctant to use commercial mobile broadband services during mission critical operations (chapter 4). PSAs have suggested that until a public safety grade service is available, they are unlikely to make widespread use of mobile broadband or undertake significant investments in mobile devices, upgrades to systems or protocols, or personnel training (ACT Emergency Services Agency, sub. 25).

The implication is that greater benefits could be realised if PSAs increased their use of mobile broadband. Many participants argued that concerted action by governments and others is needed to provide a public safety grade service that PSAs can rely on.

DRAFT FINDING 3.2

PSAs' uptake of mobile broadband applications is limited at present due to concerns about the quality of commercial mobile services. Critical issues include the ability of PSAs to get priority access to — and sufficient capacity on — commercial mobile networks during times of congestion, and the reliability of commercial networks relative to land mobile radio networks.

Governments can facilitate PSMB

PSAs represent only a small fraction of potential demand compared to the wider consumer market. In practice, the services currently on offer from commercial mobile carriers fall short of what PSAs require for mission critical situations. Although the quality of services offered by mobile carriers is likely to continue to improve in line with general market developments, there is a risk that these services do not improve to the extent that PSAs require (at least in the near term), or do not evolve in a way that facilitates interoperability among PSAs.

There is a general presumption that governments will need to intervene on behalf of their PSAs to facilitate greater adoption and take up of mobile broadband. This view was expressed by study participants and reflects actions being taken by governments in other countries to deliver mobile broadband to PSAs (appendix B).

State and territory governments could become actively involved in facilitating PSMB in a number of ways. For example, they could:

- directly fund, own and/or operate a dedicated PSMB network
- pay one or more of the commercial mobile carriers to deliver a PSMB service
- provide additional funding or other inputs (such as spectrum) to PSAs that would help them to build or purchase a mobile broadband service
- collaborate with other jurisdictions and coordinate efforts to develop technical standards and platforms for interoperability.

All these options would have benefits and costs for the community, including the costs that arise from directing resources away from alternative uses (opportunity costs). This study weighs up these benefits and costs, and considers how governments could best facilitate PSMB and the roles that PSAs will need to play in making use of it.

3.2 The Commission's first principles approach

The Commission has been asked to undertake a 'first principles' analysis to determine the most efficient, effective and economical way of delivering a PSMB capability to PSAs by 2020, giving consideration to:

- the need for the capability to be reliable and secure, nationally interoperable across jurisdictions and agencies, provide PSAs with priority access, and operate in both metropolitan and regional Australia
- the relative costs, benefits and risks of alternative options for deploying a PSMB capability — including deploying a dedicated PSMB network, an approach that is reliant on commercial networks, or some combination of the two
- relevant domestic and international reports and experiences.

Analytical approach

The Commission has approached this task through the method of cost–benefit analysis (box 3.4). Cost–benefit analysis is a tool that can be used to rigorously and consistently assess a range of options for meeting a policy objective, and in a way that encourages decision makers to take into consideration all costs and benefits of a project (PC 2014b).

In undertaking this analysis, the Commission has sought to quantify as many elements as possible. However, it is not always feasible to express non-monetary benefits and costs in dollar terms. Particularly in regard to the benefits and risks of rolling out a PSMB capability, the Commission has described likely impacts qualitatively due to lack of data.

The process used by the Commission to apply cost–benefit analysis is summarised in figure 3.2. The first stage is to develop an understanding of PSAs' mobile broadband requirements into the future, taking into account the mission critical nature of public safety work and the associated service quality requirements (chapter 4). Drawing on these insights and other evidence, the Commission has sought to identify a range of PSMB scenarios that describe the level of network capacity that a PSMB capability could deliver. A 'starting point' definition of a mission critical mobile broadband data network has also been proposed.

The next step is to consider the various ways that a PSMB capability could be delivered. Specifically, the Commission has explored — in a qualitative way — some of the technical and cost implications of relying on different inputs and deployment approaches (chapter 5).

This analysis is used to highlight some of the key drivers of costs and the tradeoffs between different deployment approaches.

Box 3.4 Cost–benefit analysis

Cost–benefit analysis (CBA) is a method that can be used to evaluate whether an investment project or a policy makes the community better off overall compared to the status quo. It involves aggregating impacts on all members of the community and appropriately taking account of risks.

In CBA, benefits are valued according to the willingness of individuals to pay for them, which is often more than they would actually pay. For example, mobile broadband could improve the services that fire agencies provide to the community, thereby reducing risks to life and property.

Similarly, costs are valued according to the willingness of an alternative purchaser to pay for the resources involved (this is called 'opportunity cost'). In other words, the inputs needed to deliver a project are measured according to the value that is forgone by not using them in other economic activities. For example, funds spent on building mobile network infrastructure would not be able to be spent on other things that the community values, such as transport or education.

Importantly, CBA takes into account the value of the service to consumers beyond the price paid, and the cost beyond what is paid to the factors of production. CBA can also take into account any externalities — other costs and benefits — that fall on people outside those involved in the transaction.

The costs and benefits of projects and policies often accrue over a considerable length of time. To reflect this, the analysis is typically conducted over a long time period, such as 20 or 30 years. To take account of people's preference to receive benefits now rather than later, future values are discounted to a present value.

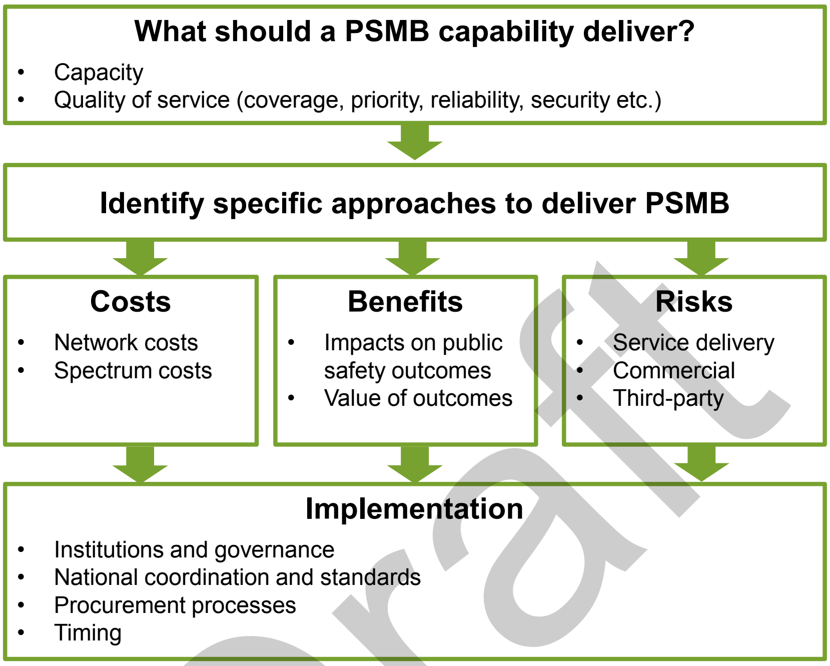
In general, projects with positive net benefits should be accepted. However, where there are mutually exclusive projects, the one with the highest net benefits should be preferred.

Sources: Baker and Ruting (2014); Department of Finance and Administration (2006); PC (2014b).

There are many ways that PSMB could be delivered, and it is not practical to undertake a detailed evaluation of every possible approach. However, important insights can be gleaned from examining a discrete set of options. To this end, the Commission has specified and evaluated a number of specific PSMB delivery options that are realistic, technically feasible and sufficiently differentiated (chapter 6). This analysis illustrates — quantitatively where possible — the costs, benefits and risks associated with each option. It also examines the implications of using different types and quantities of inputs to deliver PSMB.

There is a range of implementation issues associated with PSMB that are difficult to assess quantitatively, or to capture through a cost–benefit analysis. While some of these implementation challenges will arise regardless of how PSMB is delivered, others will vary by deployment approach. For example, the institutional and governance arrangements that underpin delivery of PSMB can affect the efficiency (or otherwise) of investment in, and operation of, PSMB networks. Implementation can also pose risks and challenges for governments, PSAs, the community and commercial providers. The Commission has examined these aspects of implementation and potential strategies that can be used to manage risk (chapter 7).

Figure 3.2 **The Commission's analytical approach**



Evaluating PSMB options

The Commission has sought to evaluate the costs, benefits and risks of various PSMB delivery options over a 20-year time horizon.

Where possible, the costs of alternative options have been evaluated in a quantitative way to show the relative importance of particular cost drivers or the magnitude of certain tradeoffs (box 3.5). The quantitative analysis is illustrative only and should be considered in the context of its limitations (discussed below). Chapter 6 and appendix C provide a fuller exposition of the approach taken to the quantitative component of the evaluation.

Box 3.5 A 'fit for purpose' quantitative analysis

This study undertakes a bottom-up quantitative analysis, involving three key steps:

- Geotyping — using ABS data to assign different geographical areas of Australia to particular geotypes (dense urban, urban, suburban, rural or remote)
- Radio Access Network dimensioning — estimating the number of mobile sites required to meet coverage and capacity requirements
- Network costing — applying benchmark cost values (such as the costs of mobile base station equipment) to calculate total capital and operating costs.

The key output from the quantitative evaluation is a net present value of the cost of each option, assuming a 20-year time horizon (2018–2037). Importantly, the exercise is not designed to:

- produce precise estimates of the total costs of individual options, or individual cost components; rather, the focus is on relativities
- describe what the architecture of a PSMB network would look like in practice
- identify (in an exact way) the optimal mix of inputs for delivering a PSMB capability.

Costs

The Commission has focused on two main components in assessing the costs of PSMB:

- network-related costs (capital and operating expenditures) (box 3.6)
- spectrum costs.

Consistent with the principles of cost–benefit analysis, each of the above components is assessed in terms of its opportunity cost (the value of the next best alternative use). It is also measured incrementally — that is, the cost of delivering a PSMB capability relative to the status quo.

Market prices are of limited use in the analysis, because the prices actually paid in markets do not always reflect the underlying costs. For example, market prices currently charged for network-related services may reflect the cost of *past* investment — or imperfections in the market — rather than the underlying cost of inputs needed to deliver a PSMB capability in *future*. The Commission's analysis is focused on these underlying input costs, regardless of who owns existing infrastructure or finances the deployment of PSMB (these matters are dealt with separately).

Spectrum costs are also difficult to value. The opportunity cost of spectrum may not always be the same as the price that is actually paid. In addition, different parcels of spectrum have different technical properties, and so their values can differ. Moreover, spectrum is auctioned by government only infrequently, and is not widely traded on secondary markets, meaning that available market prices need to be treated with caution.

Box 3.6 **Network-related costs**

A number of network-related costs have been examined in this study. Many of these differ depending on the deployment approach being analysed.

Capital costs

- Radio access network sites and equipment (including towers, antennas, power equipment)
- Site hardening costs, to improve security and reliability of a mobile network (including physical site upgrades, augmented back-up power, dual path backhaul transmission)
- Core network hardware and software (including new core deployment, network monitoring tools, Operations Support System, Business Support System, LMR network gateways)
- End-user devices (including handheld devices, in-vehicle terminals)

Operating costs

- Network-level costs (including maintenance and network management costs)
- Leasing land, equipment, facilities and services (including site acquisition and management costs)
- Renting backhaul transmission capacity

Some cost components can be interdependent. For example, the quantum of spectrum used may have a bearing on the magnitude of network costs needed to provide a given level of capability to PSAs (chapter 5). Similarly, the choice of spectrum band may influence end-user equipment costs, if only certain types of equipment (such as handsets) can be used at those frequencies.

In evaluating the costs of specific PSMB delivery options, the Commission has had to make a number of simplifying assumptions. In many cases these reflect limitations in the available data. Sensitivity analysis has been used to assess how these assumptions and data inputs affect the quantitative cost estimates, and to provide an indication of the likely range of costs where there are uncertainties.

Benefits

A mobile broadband capability does not generate benefits in its own right. Rather, it facilitates the use of various applications, which in turn can improve the efficiency and effectiveness of public safety services, leading to outcomes or improvements that the community values. The benefits of PSMB therefore hinge on how PSAs actually use the capability to deliver public safety services.

Two types of benefits are relevant for the evaluation exercise — the value of improved public safety outcomes (such as lives saved or property damage avoided), and cost savings (or productivity gains) in the delivery of public safety.

To quantify these benefits, it is necessary to:

- identify how PSAs would use a PSMB capability to change their activities, operations and procedures
- identify how these changes would impact public safety outcomes, including productivity improvements
- express the outcomes in monetary terms (a consistent unit of measurement that allows benefits to be compared with costs).

While potentially large benefits could flow from a PSMB capability, the task that has been assigned to the Commission is not limited to measuring the benefits of PSMB per se. Rather, the relevant issue for this study is whether the benefits are likely to vary between alternative PSMB deployment approaches and, if so, the nature and magnitude of those differences.

However, there are multiple challenges involved in quantitatively estimating benefits. First, it is very difficult to assess how PSMB is likely to impact on public safety outcomes. This is because these outcomes depend on a wide range of factors, including other tools that PSAs use (such as vehicles and LMR networks) as well as external influences (such as individuals' actions, the weather and crime reduction policies). Complicating this is wide variation across PSAs in the activities they undertake and where they operate, and how they will adapt their operations to make use of PSMB.

A lack of suitable data on all these factors makes measurement extremely challenging. While study participants commented that there were significant benefits to be gained from PSMB, few of them were able to follow up with documentation of those benefits. Moreover, very few publicly available studies have attempted to quantitatively estimate the benefits of PSMB, and there do not appear to be any studies that have quantitatively estimated the benefits of alternative PSMB deployment approaches.

Second, it is challenging to estimate the value the community places on different public safety outcomes, due to limited information. While it is sometimes possible to draw on existing published estimates (such as of the costs of crime or value of a 'statistical life'), few estimates are available and applying these to a different context can be fraught with error (Baker and Ruting 2014).

Third, the extent to which benefits can be confidently estimated is limited by the significant uncertainty surrounding how mobile broadband will be used by PSAs over time and how technologies will evolve. For example, there is a wide range of applications that PSAs could potentially use, some of which may not have been developed yet. This is further complicated by the coexistence of other communications technologies, such as LMR networks and satellite phones. As the NSW Telco Authority (sub. 30, p. 63) has observed:

> The lack of maturity in a PSMB both here in Australia and internationally makes undertaking a quantifiable assessment of the benefits difficult, as a result there is little material in the public

domain. Unlike costs, benefits will only be realised into the future once PSMB is available and so are difficult to quantify now.

Given these practical difficulties, the Commission has assessed the differences in benefits between approaches in a qualitative way. In effect, the Commission has undertaken a cost effectiveness analysis and supplemented this where feasible with a qualitative analysis of any differences in benefits between different delivery options. That said, because the options under evaluation have been designed to deliver a similar level of capability to PSAs, the impact of each option on public safety outcomes (and thus, its benefits) is not expected to vary markedly.

Risks

One of the main challenges in identifying and quantifying the costs and benefits of different options for delivering a PSMB capability is the high level of uncertainty surrounding the magnitude, nature and timing of the costs and benefits. There may also be high levels of risk associated with the procurement, construction and operation of a PSMB capability (chapter 6).

The Commission's evaluation is focusing on risks that are likely to differ across delivery options. These can be grouped into three main categories:

- technical risks — for example, risks relating to construction cost overruns and delays, whether the capability meets PSA requirements, availability of technology or inputs, achieving interoperability over time, service interruptions or maintenance
- commercial risks — for example, risks associated with suppliers not participating in tendering, delays in procurement, or being locked in to a specific supplier
- third-party risks — for example, the risk of adverse impacts on consumers (or other groups) arising from disruption in the quality of service they receive over mobile networks, or due to reduced competition in the market.

These risks are diverse, and do not always lend themselves to quantification. The Commission is assessing these risks qualitatively, with a focus on how they might differ across delivery options (other risks may be common across options, such as delays in governments making decisions). In doing so, the ability to partly or fully mitigate risks under each option has been taken into account.

Challenges and limitations with quantitative evaluation

The limitations with any quantitative analysis and its interpretation have long been recognised. Albert Einstein is noted for saying that 'not everything that can be counted counts, and not everything that counts can be counted'. It is a case in point for assessing the costs and benefits of PSMB.

There are several challenges with quantitatively evaluating PSMB delivery options:

- the design (or 'dimensioning') of mobile broadband networks is technically complex, and involves a wide range of considerations and inputs
- a significant amount of data would be required to quantitatively analyse all the costs and benefits of a specific PSMB option, and these data do not always exist
- even where data inputs are available, there are critical gaps, such as where information is commercially sensitive and thus cannot be publicly reported.

While the Commission is not an expert in mobile network design, it has drawn on publicly available research and analytical exercises undertaken by others. It has also sought feedback on specific elements of its analysis through technical workshops and from consultants, industry experts and commercial mobile carriers. Where commercial-in-confidence data have been received from study participants, these data have not been directly used in the quantitative analysis for reasons of transparency — doing so would make it difficult (or impossible) for the Commission's estimates to be reproduced and scrutinised. Nevertheless, these data have been helpful in forming views on specific benchmarks for various network cost components.

Additional feedback on the Commission's approach is sought so that the analysis can be further developed for the final report.

Finally, rather than attempting to identify a single best PSMB option, the Commission has sought to provide advice and guidance on key elements of PSMB deployment approaches and their implementation — including governance, procurement and the timing of investment. This guidance is robust to a range of possible circumstances. This is essential given the differing circumstances of individual jurisdictions (and PSAs), and the impracticality of a one-size-fits-all solution.

4 What is a public safety mobile broadband capability?

Key points

- A mobile broadband capability can be described in terms of the network capacity available to end users and the quality of services delivered.
  - Network capacity refers to the amount of traffic that can be transmitted on the network at any given time and is often measured in bits per second.
  - Service quality has several dimensions (or characteristics), including coverage, reliability, security and interoperability.
- There is no single definition of a 'public safety grade' mobile broadband capability — a range of capacity levels and service quality standards could feasibly apply.
  - Public safety agency (PSA) demand for communications services increases significantly during emergency incidents (peak periods) relative to 'business as usual' periods. It is unlikely to be economic to provision a public safety mobile broadband (PSMB) capability to cater for relatively infrequent peak events.
  - Not all PSA demand needs to be met in real time. Demand management by PSAs is crucial to ensuring the net benefits of a PSMB capability are maximised.
  - The 'mission critical' nature of public safety activities means PSAs require a higher quality of service relative to other mobile customers.
- PSAs' future demand for mobile broadband network capacity is highly uncertain, as are the benefits of that use. Demand will depend on a complex range of factors, including the prices that PSAs face, the availability of alternative communications systems and technological developments. Attempts to generate a quantitative, 'bottom up' estimate or projection of demand would be extremely data intensive and unlikely to yield robust results.
- There is broad agreement that a PSMB capability should be of sufficient quality to support the use of mobile data applications in mission critical situations. However, operationalising the concept of a mission critical data network is difficult — evidence on the specific service standards required is sparse and inconsistent.
- The level of network capacity and service quality made available to PSAs should reflect the particular circumstances of individual jurisdictions — there is no 'one size fits all' solution.
- PSMB scenarios have been developed to facilitate the quantitative analysis. These scenarios allow delivery options to be assessed on an even keel and the cost implications of provisioning for different levels of network capacity to be illustrated.

A mobile broadband capability has two important dimensions — the quantity of mobile broadband services (or network capacity) available to end users and the quality of those services (section 4.1).

The key task for this study is to identify the best way to deliver a 'public safety grade' mobile broadband capability. What this means in practice is somewhat subjective; definitions vary and study participants presented a range of views. However, given the task at hand, it is useful to consider — at least in a broad way — what the capacity and quality dimensions of a public safety mobile broadband (PSMB) capability might look like.

A useful starting point is to consider the unique responsibilities and activities of public safety agencies (PSAs), and the role of mobile broadband communications in delivering public safety services (section 4.2). Detailed information about what PSAs are seeking from a mobile broadband service, including their willingness to pay (or demand), would also be useful. However, publicly available information is sparse, and there is significant uncertainty (section 4.3).

This notwithstanding, PSMB scenarios can be used to highlight the relative merits of different deployment approaches (dedicated, commercial or hybrid) (section 4.4). Scenario analysis can also illustrate the cost implications of provisioning for different levels of network capacity. Ultimately, however, jurisdictions will need to decide what level of network capacity and service quality is in their best interests, taking into account the costs and benefits to the community as a whole.

4.1 Key dimensions of a mobile broadband capability

Quantity (or network capacity)

The 'quantity' of services that a mobile broadband capability provides is often described in terms of network capacity, though a number of other terms are also relevant (box 4.1). Capacity refers to the speed and volume of data that can be transmitted through a mobile network and is dependent on a range of factors. It can be measured in terms of bits per second (bps) available to end users at a given time and location (a speed or 'flow' measure), or in terms of the amount of data that can be transmitted over a given period of time (a volume or 'stock' measure). Capacity is of prime importance to mobile users because it determines the type and amount of mobile applications that can be used.

Many study participants have pointed to the importance of a PSMB capability providing sufficient capacity to public safety officers, particularly during periods of peak demand when networks become congested. However, as discussed in section 4.3, evidence on what this means for the level of network capacity required as part of a PSMB capability is sparse.

Box 4.1 Measuring the quantity of mobile broadband services

The capacity or throughput of a mobile network refers to the speed and volume of data that can be transmitted on the network at any given time.

Network capacity is dependent on a range of factors, including the technology used, and the type and amount of spectrum available (Ernst & Young 2011). The amount of capacity that an individual user can access at any point in time is affected by additional factors, including their distance from the nearest mobile tower or base station, environmental and topographical factors, and the type of device they are using (chapter 5).

Network capacity can be measured as a 'flow' (or speed), for example:

- kilobits per second (kbps): 1 kbps = 1000 bps
- megabits per second (Mbps): 1 Mbps = 1000 kbps
- gigabits per second (Gbps): 1 Gbps = 1000 Mbps
- terabits per second (Tbps): 1 Tbps = 1000 Gbps.

Stock measurements of mobile broadband networks are also used, such as the total volume of data used over a given period of time (for example, gigabytes or terabytes per year).

Mobile network capacity has two elements: uplink capacity and downlink capacity. The uplink capacity determines how much data end users can send (for PSAs, this could be field officers sending information about a scene or victims to other field officers or to central command). The downlink capacity determines how much data end users can receive (such as patient medical records or maps). PSAs tend to have a high demand for uplink capacity, and exhibit a higher uplink–downlink ratio, relative to other mobile customers. This reflects the need for officers to transmit information and evidence from incident scenes back to central command (Alcatel-Lucent, sub. 15).

Quality

A number of dimensions (or characteristics) of mobile broadband service quality are important to PSAs. The terms of reference specify that the Commission is to give explicit consideration to these characteristics in identifying the best way to deliver a PSMB capability.

Accessibility

Accessibility refers to the ability of PSAs to get on to a mobile network. Many study participants considered that PSAs need 'guaranteed' access to PSMB networks, irrespective of the level of congestion.

Network accessibility is of most concern to PSAs when they rely on commercial networks for mobile broadband services. In this circumstance, a surge in demand from the general public can make it difficult for users to get on to the network (for example, on New Year's

Eve). Moreover, because commercial parties operate these networks, PSAs do not usually have any control over which users are (or are not) granted access.

Contracts between PSAs and the commercial carriers that 'guarantee' network access could potentially mitigate this risk. However, the Commission is not aware of any such arrangements being in place (chapter 5).

Accessibility could also be an issue for PSAs on a dedicated (or standalone) mobile network, for example, if a large incident means it is not possible for all officers to be granted access to the network when it is needed. Indeed, over-subscription is an issue that occasionally arises on land mobile radio (LMR) networks. While PSAs themselves would be responsible for determining who gets access in this circumstance, there are technical and operational challenges associated with achieving this, especially where networks are shared between multiple agencies and/or 'real time' (dynamic) adjustments are required (box 4.2 and chapter 5).

User prioritisation

User prioritisation refers to systems that prioritise certain PSA officers, devices or applications over other mobile traffic on a network. As a service quality characteristic, it is closely related to accessibility — once PSAs obtain access to a network, they also need assurance that their demand for capacity will be prioritised (or given precedence) over other users. From a network operation perspective, user prioritisation can be achieved in different ways, including by reducing the amount of capacity available to other users (slowing down network access) or by 'load shedding' (or 'pre-emption' — that is, dropping some users off the network during high-traffic periods on a priority basis).

Motorola (sub. 12, p. 23) pointed to the importance of user prioritisation being achieved in real time.

> 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. … 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.

At present, PSAs using commercial mobile broadband services for data are typically afforded only the same priority as other users, despite 4G technology offering the potential to prioritise certain users over others (chapter 5).

Box 4.2 What does it mean to guarantee accessibility and priority for public safety users?

Most public safety agencies (PSAs) are seeking a mobile broadband service that delivers ‘guaranteed’ network access, and prioritises PSA traffic over other traffic. There are various ways that these requirements could be operationalised.

Static or dynamic accessibility and prioritisation

Static (or ‘default’) access and priority arrangements are determined based on the long-term needs of PSAs (that is, considering business as usual activities and possible emergency activities). For example, each PSA user might be allocated a particular profile or status, which determines how access and network capacity are allocated.

Dynamic access and priority are where the default arrangements are able to be changed in real time, potentially facilitating a more efficient response to unfolding emergency incidents (for example, if the nature and location of an incident render the default settings sub-optimal). A dynamic change could be triggered by various means, such as end-users pressing an emergency button on their device or turning on vehicle lights and sirens.

Access and priority on the basis of agency, user, device or application

Access and priority could be determined on the basis of the agency, the public safety officer, the device or the application. For example, mission critical voice applications could be given precedence over data applications and low priority voice, or location services and dispatch messaging could take precedence over video and file transfers. Assigning priority on the basis of device might also be desirable, such as for PSA workforces that are highly volunteer dependent, or subject to churn. This approach might also suit in-vehicle devices, which have multiple users.

How should accessibility and prioritisation mechanisms be controlled?

A somewhat contentious issue regarding dynamic access and priority mechanisms is who is made responsible for administering them, and who has the authority to initiate or implement dynamic changes. As noted above, it may sometimes be desirable for public safety officers themselves to have the ability to trigger access and priority changes. In other cases, it may be more practical for an authorised administrator, dispatcher or incident commander to be the sole custodian of dynamic changes.

Can access and priority be ‘guaranteed’?

In practice, it is not feasible to guarantee that a particular service standard will be met 100 per cent of the time. For this reason, service level commitments are typically defined in terms of an acceptable performance standard (for example, access to be provided 99.9 per cent of the time), or an acceptable risk of failure (less than 0.1 per cent). The same is expected to be true of access and priority mechanisms, meaning some acceptable level of failure would need to be specified.

Source: NPSTC (2012).

Coverage

The coverage of mobile broadband networks is important to PSAs because it determines where in Australia they are able to access mobile broadband.

PSAs are responsible for protecting people, property (such as buildings, power stations and gas pipelines) and land (such as state forests and national parks). This means PSAs operate across a vast geographic area, including major population centres, rural, regional and remote communities, unpopulated areas and at sea. The ability of PSAs to use communications systems in these areas is dependent on the coverage of the underlying networks.

Network coverage can be measured in two ways: by estimating the percentage of the population that resides in the coverage area, or by estimating the land area or road distance covered by a network.[1] Both of these coverage measures are important to PSAs, and many participants considered that a PSMB capability should have the same network and geographic coverage as LMR networks (discussed below). The ability for public safety officers to access mobile broadband services indoors and underground has also been raised as an issue (Telstra, sub. 19).

Reliability (or resilience)

In broad terms, network reliability (or resilience) refers to the ability of the network to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation (ENISA 2011; NPSTC 2014). Network reliability is often measured in terms of:

- availability — the minimum percentage of time the network is functioning (or the maximum number of hours per year it is unavailable due to faults or unplanned outages)
- network recovery time — the maximum time it takes to rectify faults and outages (such as mean down time, or mean time to repair, measured in hours).

Network availability is important to all network operators (and users), including the commercial carriers. Indeed, commercial network outages can lead to revenue loss, reputation risk and loss of customers. However, a number of study participants considered that the reliability levels of commercial networks are too low to support public safety services, and do not match those of LMR networks.

1 Each of these calculations can be done in multiple ways, giving rise to potentially different coverage levels for a given network.

The Australian Radio Communications Industry Association noted:

> Anecdotal evidence from major incidents, both within Australia and internationally, is that often the narrow-band systems continue to operate long after other communications systems fail. (ARCIA, sub. 2, p. 13)

As noted in chapter 2, during the 2015 Hunter Valley floods and the 2014 Warrnambool exchange fire (box 4.3), LMR networks continued to operate despite one or more of the commercial networks being unavailable.

Security

The data and information generated, stored and exchanged by PSAs is often highly sensitive and confidential. Protecting this information from disruption, interception and misuse is critical to the integrity of PSAs' operations and the privacy of individuals. For these reasons, PSAs typically require a more secure communication service than most commercial users.

The security of the *physical* network infrastructure is also important to PSAs. This means that network infrastructure is protected from malicious intent or natural events that could disrupt operation. An example of how the physical security of telecommunications infrastructure can be compromised is provided in box 4.3. Motorola (sub. 12, p. 20) noted that:

> 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.).

Box 4.3 **Warrnambool Telstra exchange fire**

In November 2012, the Telstra telephone exchange at Warrnambool, in south-west Victoria, caught on fire due to an electrical malfunction. The exchange acts as a transmission hub for telecommunications, connecting about 100 000 people over a 15 000 square kilometre area. The exchange is an example of an 'infrastructure single point of failure':

> The trade-off between improved network resilience and the practicalities of network design and operation often leads to compromises that may result in the strategic acceptance of single points of failure existing within a network. (Gregory et al. 2014)

The fire caused significant damage to essential telecommunication equipment and had an immediate impact on the Telstra mobile network. Telephone, internet, mobile broadband, business services (for example, banking) and emergency services (including 000) were disrupted. Optus' 2G mobile network was also affected; however, its 3G network remained fully operational.

Sources: ACCAN (2014); Gregory et al. (2014); Optus (sub. 18).

The security of communications services and physical network infrastructure is typically described in terms of the techniques, strategies and infrastructure that are in place to uphold security. For example, communications security can be achieved through end-to-end encryption of voice and data communications (chapter 5).

Interoperability

Interoperability refers to the ability of users to communicate by terminal device with whomever they need, when they need, when authorised. Historically, one of the main limitations of LMR networks has been a lack of interoperability between different agencies and jurisdictions (chapter 2). Inquiries following the Victorian bushfires in 2009 and the Queensland floods in 2011 highlighted that the interoperability of LMR networks is often poor and can limit the effectiveness and efficiency of PSA activities.

This issue is being addressed through the *National Framework to Improve Government Radiocommunications Interoperability*, endorsed by COAG in 2009. The objective of the framework is to transition all PSA narrowband (LMR) radiocommunications equipment to interoperable systems, modes and frequencies in the 400 MHz spectrum band by 2020 (COAG 2009).

PSAs and policy makers regard mobile communications interoperability as crucial to achieving coordinated and efficient public safety services. In broad terms, mobile broadband interoperability implies that PSAs are able to continuously share data communications with other agencies — within and across jurisdictions — during multi-agency and/or widespread incidents.

In practice, achieving interoperability is about more than the technology solution. For example, Victoria Police (sub. 17, p. 11) highlighted that interoperability depends on 'governance, training, and standard operating procedures', and cautioned that:

> without a National Governance Structure the opportunity will be lost to truly operate nationally in a joined up manner, and deliver such broadband capabilities within and across borders in an unfettered secure and resilient manner.

Institutional barriers to interoperability are discussed in chapter 7.

Device compatibility

A key issue for many PSAs is the ability of officers to access mobile broadband using a wide range of field equipment, including 'off-the-shelf' handsets (smart phones, tablets and laptops), customised handsets and other equipment that supports mobile broadband applications (for example, communication devices in ambulances or police cars).

Participants stressed that such flexibility is important for containing the device costs faced by PSAs, accommodating the sizable volunteer base within the emergency management sector, and facilitating PSAs' uptake of mobile broadband applications (and the benefits that flow from this). Indeed, Rivada Networks (sub. 9, p. 16) considered that PSAs 'cannot evolve efficiently if they are burdened with paying a premium for specialised devices that are not offered with the benefits of commercial economies of scale'.

Voice integration

Voice (delivered over LMR networks) is the principal way that PSAs communicate. A range of voice services and applications are relied upon heavily by PSAs, including push to talk (PTT), one-to-many communications (group calls and talk groups), dispatch and emergency alerting (chapter 2).

In the future, it is likely that PSAs will want to consolidate voice and high speed data traffic onto a single network. However, when and whether this happens will depend on a range of factors, including the ability of mobile broadband networks to integrate (and deliver) the voice services that PSAs rely upon to an equivalent or better quality (relative to LMR) and the lifecycles of existing LMR infrastructure and systems.

Various characteristics of voice service quality are important to PSAs, especially during 'mission critical' situations, including:

- latency, that is, the time taken to initiate communications (such as how quickly a user can talk on the system after pushing a button), and how soon others receive the transmission. In narrowband LMR systems, any talk group member can initiate a group call via a single button press and the call is established in less than half a second (TETRA MoU Association 2004)
- the quality and integrity of the audio that is transmitted. For example, in mission critical situations, the listener must be able to understand without repetition, identify the speaker, detect stress in a speaker's voice, hear background sounds and so on
- the ability to operate PTT one-handed. Some applications developed for smartphones require users to hold the phone in one hand and push a button on the touch screen. This may not be acceptable for certain roles and circumstances affecting public safety officers.

The latency of data services (such as real-time video) delivered over PSMB is also important to PSAs. In this context, latency refers to the time it takes for a packet of data to be delivered to its destination and is usually measured in milliseconds. In practice, data packets can be held up in long queues, or take a less direct route to avoid congestion, increasing latency. This delay can build up over time, even if the throughput rate is normal.

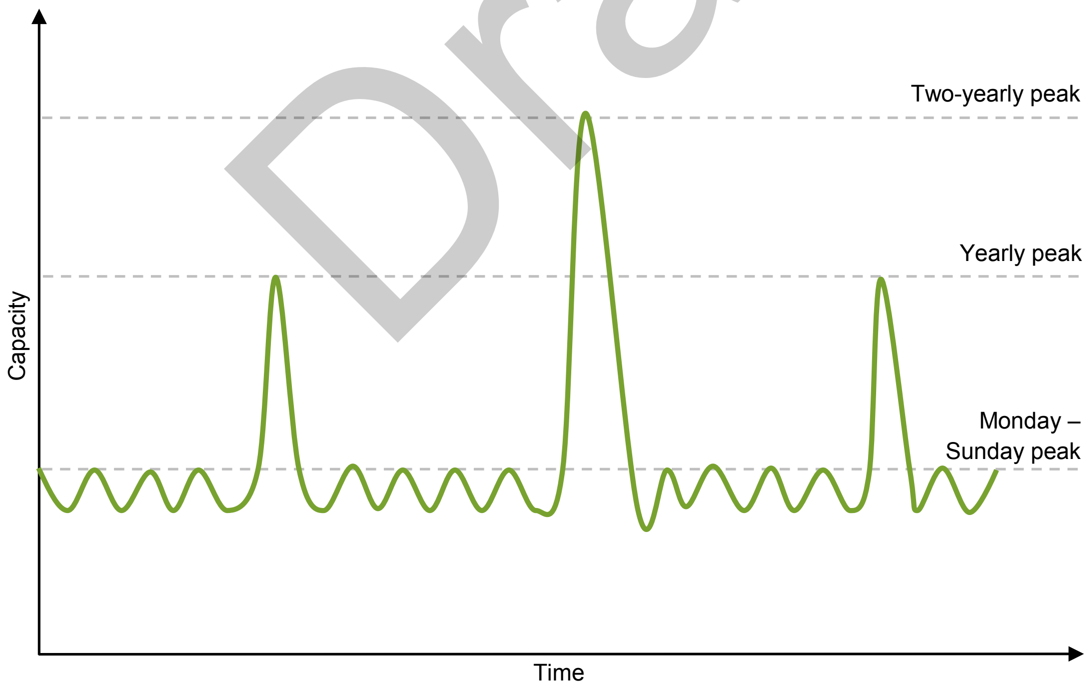
4.2 How are PSAs different to other mobile broadband customers?

The distinct nature of PSAs' activities and their demand for mobile broadband services (and communications services more generally) is important for considering the amount of network capacity, and the quality of service, that a PSMB capability should deliver. ('Demand', as it is described here, does *not* refer to how PSAs' network usage relates to price or 'willingness to pay'; it is therefore not a true measure of demand, as economists usually define it.)

PSA demand for mobile broadband is 'peaky'

The network capacity that any PSA or officer requires will vary over the course of a day, month or year. Broadly speaking, PSAs' activities (and their corresponding communications needs) can be classified into 'business as usual' (BAU) periods and peak periods (figure 4.1).

Figure 4.1 **Stylised PSA demand profile**



BAU periods are those where PSAs undertake routine tasks, such as transporting patients between hospitals or conducting roadside breath testing. Peak periods refer to times where PSAs are responding to emergency incidents or large planned events, in addition to BAU. Peak periods can include relatively minor emergencies (a traffic accident or house fire), major or wide-scale emergencies (a natural disaster or hostage situation) and large planned events (AFL Grand Final Day or the Darwin Cup).

The capacity requirements of PSAs are expected to remain fairly stable and predictable during BAU periods, but surge suddenly and (potentially) significantly when PSA activities peak. That said, the unique features of particular agencies mean that no two PSAs share the same demand profile — for example, police tend to have higher BAU demand relative to fire agencies, given the large volume of non-emergency activity (proactive patrols, community policing and so on) that police undertake (NSW Telco Authority, sub. 30; SCF Associates 2014).

Participants also pointed out that PSAs' use of mobile broadband services during BAU periods is growing rapidly, as agencies gain experience with mobile broadband technology and embed mobile devices and applications in their day-to-day operations (MFB, sub. 6). PSAs' future mobile broadband needs are discussed in section 4.3.

Peaks are large (relative to 'business as usual') and unpredictable

General (non-PSA) mobile traffic also comprises BAU and peak periods. However, the traffic profile of PSAs can be distinguished from general mobile broadband traffic in two respects.

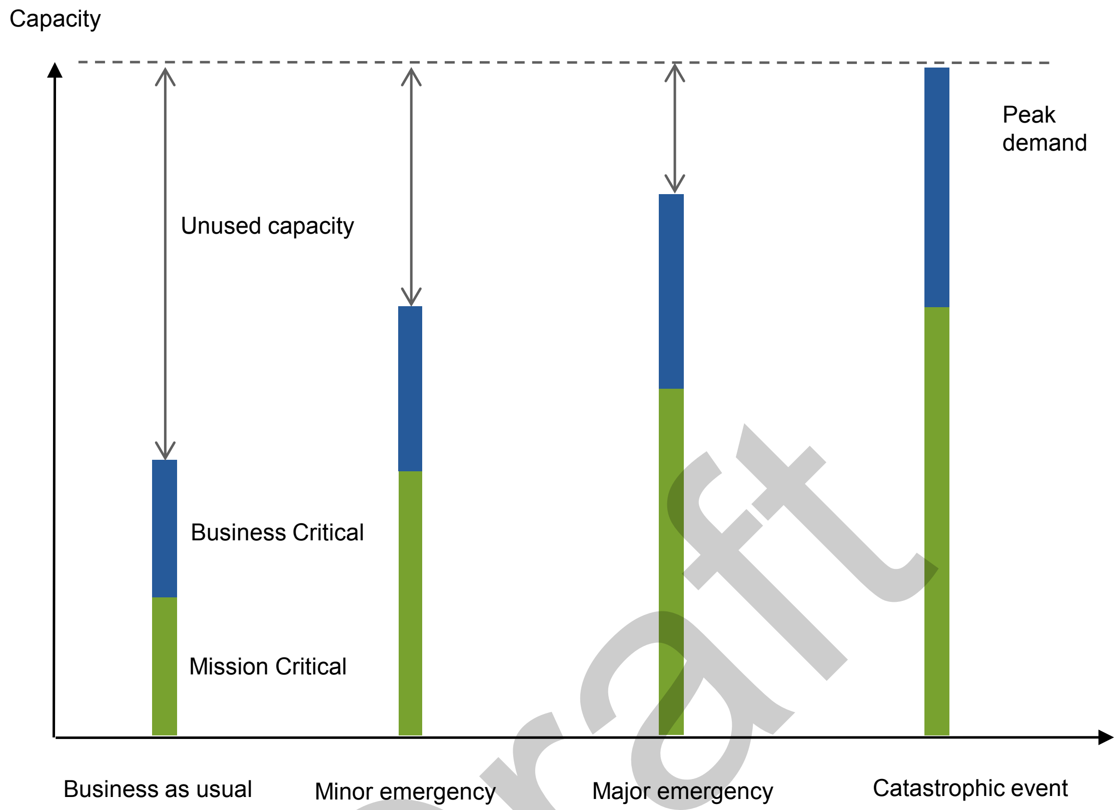
First, the difference between demand during BAU periods and peak periods is large relative to other mobile broadband customers. For example, Alcatel-Lucent (sub. 15, p. 4) observed that:

> PSA communications networks will typically demonstrate a significantly greater discrepancy between average everyday demand and peak demand than in a commercial network. In Alcatel-Lucent's experience, current peak PSA communications traffic in times of crisis and emergency is typically 10-to-20 times larger than average demand as PSAs focus their attention on a particular location and/or event.

Second, many peak demand periods for PSAs are unpredictable in timing, location, severity and incidence (as is the nature of crisis and emergency). Usage patterns of commercial mobile customers are relatively easier to predict by comparison, drawing on historical experience for when key surges in demand take place (for example, Friday and Saturday nights, New Year's Eve and during major sporting events).

These features have implications for the development of PSMB options, and the planning and design of PSMB networks (often referred to as 'network dimensioning', chapter 5). In particular, deploying a (permanent) PSMB network to meet demand during relatively infrequent and unpredictable peak events would lead to very low levels of capacity utilisation (figure 4.2) and high marginal costs per megabyte of data transmitted, likely making it uneconomic. Indeed, commercial mobile networks are typically designed to deliver some estimate of 'busy hour' traffic over a typical week or month (box 4.4), not demand during infrequent peak events.

Figure 4.2 **Meeting peak demand implies significant network capacity**



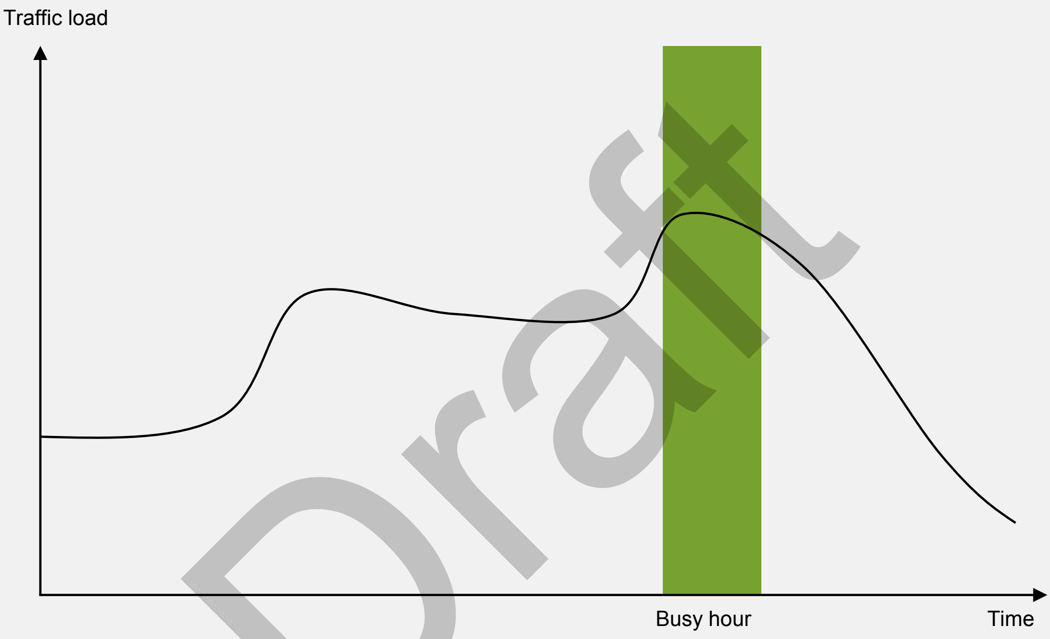
Dimensioning a mobile network to meet lower levels of demand does not necessarily mean that PSMB networks would be severely congested during peak periods, or that important demand would go unmet. There are strategies that can be used to provide PSAs with temporary coverage and capacity (such as cells on wheels) (chapter 5) and techniques are available to PSAs to manage their demands on a network during peak periods.

In particular, some PSA communications during peak periods are not necessarily high priority, and may be able to be shifted to other time periods without any significant loss. This is true of some voice communications currently delivered over LMR networks, and the same is expected to be true for mobile broadband communications. Strategies can also be employed to reduce PSAs' demand for mobile broadband capacity during peak periods, such as 'store and forward' or 'compression and broadcast' of video-based applications, or offloading traffic to alternative networks (fixed or Wi-Fi). Appropriate pricing frameworks can ensure that PSAs are encouraged to pursue these options where it is more efficient than using network capacity (chapter 7).

Box 4.4 What is the 'busy hour'?

In mobile networks, the 'busy hour' is the 60-minute period during which mobile network usage is at its highest in a given period (a day or a week, for example). The busy hour might well occur at different times in different regions of Australia. A single user can potentially contribute to two or more busy hours — in their home location (where the busy hour might occur in the evening) and in the place they commute to for work or education (where the busy hour might occur in the daytime).

Commercial mobile networks are typically dimensioned to meet a carrier's assessment of average or normal 'busy hour' traffic. This might be calculated by averaging the busy hours for each day over a week, month or year.



DRAFT FINDING 4.1

The communications needs of PSAs are characterised by high and non-predictable peak periods. PSAs can (and do) employ strategies to reduce their demands on communications networks during peak periods without any significant loss of benefits. Provisioning a PSMB network to meet relatively infrequent peak events would be prohibitively expensive.

The mission critical nature of PSA work drives high quality of service requirements

PSAs rely on communications systems for most (if not all) of their activities, some of which are regarded as mission critical.

What is mission critical?

The term 'mission critical' has many meanings. A mission critical situation, for example, could refer to PSA activities or operations where reliable communications are necessary to avoid loss of life, serious injury or significant damage to valuable or strategic assets (NSW Telco Authority, sub. 30). Mission critical is also used to describe certain properties of communications systems (such as resilience, priority and security) that make them appropriate for use in PSA operations.

What is meant by a mission critical LMR voice network is relatively well accepted (although not necessarily universally defined). For example, Motorola (sub. 12, p. 7) suggested that a mobile radio communications system must fulfil four key requirements in order to be considered mission critical:

- The infrastructure must be resilient, redundant and highly available.
- Communication must be reliable.
- Communication must be secure.
- Point-to-multipoint communication must be supported.

What is implied by a mission critical mobile broadband data network is less clear. Some consider that a mission critical mobile network is one that — should it fail — would 'place public order or public safety and security at immediate risk', and could potentially cause loss of life (TCCA 2013a, p. 7). Others define mission critical mobile networks as those which are 'durable, resilient and effective in all situations and conditions', thereby allowing frontline officers to successfully respond to emergencies (ARCIA sub. 2, p. 4).

For this study, the Commission has used 'mission critical' to refer to PSA activities or situations where lives are on the line (that is, where there is a material risk of loss of life or severe injury), which could occur during BAU or peak periods.

Although this definition could be broadened (to include property damage, for example), it would not have significant implications for the analysis. This is because it is assumed that PSA communications systems should be able to cope with mission critical situations as a matter of course (section 4.4). Mobile broadband services that function when lives are on the line would presumably also be sufficient where property damage is likely.

Implications for service quality

The mission critical nature of public safety operations means that the quality of mobile broadband services (and indeed, the quality of all communications services that agencies rely upon) is paramount. In particular, it means that PSAs require a higher level of service — across most, if not all quality characteristics — than other mobile customers. This reflects the high benefits of reliable communications during mission critical events and the potentially dire consequences of communications systems failing.

While not all PSA activity is mission critical (such as routine or administrative tasks that may be considered operational, informational or business critical), it is not practical to offer PSAs a 'two-tiered service'. Mission critical situations are difficult to predict in advance and situations can escalate to mission critical as circumstances change. For these reasons, PSAs require that their communications systems have the capacity to be used in mission critical situations as a matter of course.

The quality standards implied by a mission critical mobile broadband data capability are considered further in section 4.4.

4.3 What do PSAs want from a PSMB capability?

If jurisdictions choose to facilitate the delivery of a PSMB capability, decisions will need to be made about the level of network capacity and standard of service that the capability should deliver.

One way to begin this task is to consider what PSAs are seeking from a mobile broadband capability. In practice, this information is imperfect, and does not necessarily reflect PSAs' (or the community's) willingness to pay for PSMB. However, it does shed light on some of the priority issues for PSAs, and the importance of taking a flexible and incremental approach to implementing a PSMB capability.

There are limited data about PSAs' future use of mobile broadband services and applications

There is widespread agreement among study participants and other stakeholders that PSAs' use of mobile broadband would increase significantly if a public safety grade service were available — particularly in terms of uplink, and largely driven by video-based applications.

For example, the Victorian Government (sub. 28, p. 20) observed that PSAs' data consumption has increased rapidly in recent years, and considered that demand would grow further with a PSMB capability.

> With the rapidly changing technological landscape, data consumption has grown significantly … [However] PSA responders are unable to leverage broadband data capabilities that are

> widely available in the community to improve service delivery (and reduce the risk of impacts from emergency events) … With greater availability of mobile broadband networks, content-rich information can be shared, including real-time video, enhanced location tracking, interactive maps and two-way messaging.

However, detailed information about how PSAs would use this service (including the type, composition and volume of mobile applications) is lacking, as is information about the benefits of that use. While some estimates exist, they are often not publicly available, or are from international sources that cannot be easily translated to the Australian context. Moreover, the rapidly evolving nature of mobile broadband technology means that existing work tends to 'age' fairly quickly. Evidence presented throughout the course of this study has thus far been limited to anecdotes or very rough proxy measures — participants discussed increasing demand in a qualitative sense, but provided little quantitative guidance on future demand.

Submissions provide some insights

A report by Gibson Quai AAS Consulting (now UXC Consulting) in 2011 to the Public Safety Mobile Broadband Steering Committee of COAG used a 'bottom up' approach to estimate how Australian PSAs might use mobile broadband in the future, using a number of hypothetical incident scenarios (GQ-AAS 2011b).

Almost all figures and calculations have been redacted in the publicly available version of this report. However, the Victorian Government, in its submission to this study (sub. 28), cited some demand estimates from a Public Safety Mobile Broadband Steering Committee report that draws on the Gibson Quai AAS work (box 4.5). This gives a sense of the potential size of PSAs' mobile broadband needs during particular incidents. However, it is difficult to interrogate these estimates (as the underlying analysis is not available), or to understand how demand might evolve in different incidents or regions. Moreover, this report found that PSAs' future mobile broadband requirements were highly uncertain, given their use of mobile broadband was only in its infancy. This suggests that these figures — now four years old — should be treated with some caution.

The NSW Telco Authority (sub. 30) is currently examining the costs and benefits of a PSMB capability for that state. As part of this work, the Authority has made some assumptions about the required levels of network capacity, including that:

- a minimum 'cell edge' data rate of 256 kilobits per second (kbps) should be provided. The cell edge data rate refers to the amount of capacity a user located at the edge of the cell (the furthest point from a mobile tower) could expect to experience (chapter 5).
- higher levels of capacity should be available towards the centre of the cell (up to 10 megabits per second (Mbps)).

These assumptions have been taken into account in the development of the Commission's PSMB scenarios, as discussed in section 4.4.

Box 4.5 Estimates of PSA demand for mobile broadband

The Victorian Government submission to this study cites demand estimates from a 2011 report of the Public Safety Mobile Broadband Steering Committee (PSMBSC). The estimates refer to anticipated PSA demand for uplink capacity in high-usage areas (such as inner Sydney) by 2020. Three estimates are provided:

- business as usual demand of 40 megabits per second (Mbps) over 180 km^2, assuming 3600 mobile units in operation
- planned event demand of 67 Mbps over 180 km^2, assuming 4000 mobile units in operation
- large scale incident demand in excess of 200 Mbps over 50 km^2, assuming 870 mobile units in operation, and 30 per cent of units transmitting video during the peak periods of the incident.

As discussed in section 4.4, the Commission's quantitative analysis focuses on PSAs' network requirements on a per square kilometre basis. It is useful, therefore, to convert the estimates cited by the Victorian Government to a $Mbps/km^2$ metric. The Commission estimates that the PSMBSC figures are approximately equivalent to an average (over the relevant network area) of:

- business as usual demand of 0.22 $Mbps/km^2$ uplink
- planned event demand of 0.37 $Mbps/km^2$ uplink
- large scale incident demand of 4.00 $Mbps/km^2$ uplink.

Source: Victorian Government (sub. 28).

Many other countries are at a similar point to Australia

Some work on PSMB has been completed in other countries. However, many countries are at a broadly similar point to Australia — that is, contemplating, planning and in some cases beginning to implement a mobile broadband capability for PSAs (appendix B). To the Commission's knowledge, there is currently no example of a 'public safety grade' mobile broadband capability in operation anywhere in the world (and accordingly, no data on how PSAs use such a capability). Moreover, attempts by foreign governments to robustly estimate PSAs' future demand for PSMB confront many of the same challenges experienced in Australia (discussed below).

That said, there is some limited information available from the United States and Canada regarding PSAs' expected network capacity requirements. This information may be relevant for considering how a PSMB capability could be defined in the Australian context (section 4.4).

The US Government is planning to build and operate a nationwide 4G network exclusively for PSAs. A government authority (FirstNet) has been established to manage the delivery and operation of the dedicated network (appendix B). The Statement of Objectives suggests that the FirstNet project is to provide network capacity of between 0.1 and 3.0 Mbps per square mile (equivalent to about 0.04 to 1.16 Mbps per square kilometre), depending on the population density of the area and other characteristics (FirstNet 2015c). This network is yet to be deployed, meaning actual capacity levels could vary.

The Canadian Government is also looking to establish a PSMB capability (appendix B). Work undertaken by the Centre for Security Science (part of Defence Research and Development Canada) in 2011 included some estimates of PSA demand for mobile broadband network capacity, based on illustrative scenarios (box 4.6).

Box 4.6 **PSMB demand estimates for Canada**

In 2011, the Centre for Security Science (part of Defence Research and Development Canada) conducted a technical assessment of the 700 MHz spectrum requirements for mobile broadband data communications. In consultation with PSAs and other stakeholders, it developed three incident scenarios to assess data throughput and application requirements:

- a severe multi-vehicle accident
- a chemical plant explosion and fire
- a sports event riot.

The report does not provide disaggregated data. However, demand profiles are presented which suggest that in the first year, total uplink demand (across all PSAs) would be about:

- 5 Mbps during a multivehicle accident
- 7.5 Mbps during a chemical plant explosion
- 10 Mbps during a sports event riot.

These estimates include PSA demand for mobile data communications for day-to-day operations (such as for the issuing of traffic notices, patrols and incident reporting).

By making some assumptions about the geographic area over which these incidents take place, it is possible to convert these estimates to Mbps/km^2 (the metric used by the Commission in this study, section 4.4). Specifically, assuming that the public safety activities associated with a multi-vehicle accident are contained within a 1 km^2 area, while the chemical plant explosion and sports event riot affect a 2 km^2 area, the respective equivalent demand estimates are 5 Mbps/km^2, 3.75 Mbps/km^2 and 5 Mbps/km^2.

Source: CSS (2011).

The UK Government is in the process of procuring a PSMB capability (the Emergency Services Network) from commercial mobile carriers (appendix B). However, little information is publicly available regarding the network capacity, or standard of mobile service, to be provided to PSAs. The tender process is expected to be completed in late 2015.

It has proven difficult to obtain data on PSAs current use of mobile broadband services

PSAs are already using a range of mobile data services, including low-bandwidth services provided over LMR networks (predominantly messaging and paging), and some commercial broadband services provided over commercial networks (for example, Queensland Police's QLite application over the Telstra network, and Victoria Police's ability to roam between the Mobile Data Network and commercial networks).

Information on the quantity and quality of data services currently being used by PSAs could be a useful starting point for defining a PSMB capability — specifically, it could put a 'floor' or minimum on the level of mobile broadband capability that is required.

However, this information has not been provided to the Commission through submissions, and is generally not available publicly. One exception is some information published by Victoria's Emergency Services Telecommunications Authority on data consumption over the Mobile Data Network (which is predominantly used for dispatch, database checks and automatic vehicle location) (ESTA 2014b). This shows that Victorian PSAs are currently consuming about 1.5 Gigabytes (GB) of data per month over this network. However, this is projected to grow exponentially in the next five years, to nearly 3.5 GB per month by 2018 — a 15 to 20 per cent growth rate per year (Weiss 2015).

A request for information regarding PSAs' current use of mobile data (and other matters) was circulated to state and territory governments in May 2015. Responses were limited, though information provided by Tasmania suggests that some PSAs are consuming relatively significant amounts of data over commercial mobile broadband networks.

In 2013-14, Tasmania Police deployed over 1000 tablet devices to its frontline police officers, replacing police desktop computers and in-car mobile data terminals (Acer Computer 2014). The Tasmanian Government has indicated that traffic over these tablets is currently about 1 GB per month per device, which is expected to increase with additional in-field video demands (Tasmanian Department of Premier and Cabinet, pers. comm., 7 September 2015).

Some agencies have expressed a reluctance to disclose information on current usage because it does not capture PSAs' 'latent' demand for mobile broadband services. In other words, because usage is constrained by the capacity of LMR data networks, and quality concerns associated with commercial networks, data usage is low and not indicative of how demand would evolve if a PSMB capability were available. Indeed, the Victorian figure described above (1.5 GB per month) is equivalent to about 4.5 kbps or 0.3 bps/km^2, which implies only very low bandwidth applications (such as vehicle tracking) are being used. This conversion is based on certain assumptions, including that the Mobile Data Network land area is approximately 17 000 km^2 (GQ-AAS 2011a). In practice, the majority of traffic probably occurs in a small portion of the network and at certain times of the day. However, even then levels of data use per square kilometre would be very low.

DRAFT FINDING 4.2

PSAs' use of mobile broadband services and applications would likely increase significantly if a PSMB capability were available. However, the level of network capacity that PSAs would use is highly uncertain, as are the benefits of that use.

A detailed, 'bottom up' estimate of PSA demand for network capacity is not feasible

In practice, no two PSAs are the same — their capacity requirements are likely to vary across locations and incidents, and grow and evolve in different ways and at different rates. For this reason, a rigorous, bottom-up approach to estimating demand would need to consider the particular needs of every individual agency.

This would involve categorising each agency's activities into different types of incidents, and then — for each type of incident — collecting data on:

- the number of end-user devices expected to be used at the incident (including handheld, vehicle-mounted and so on)
- the mobile broadband applications that would be used on each device (such as voice calls, database access or real time video feeds)
- the upload and download requirements of each application
- how many applications would be used simultaneously.

The results could then be aggregated into a weighted sum of annual traffic requirements across all types of PSA activities and across all PSAs (assuming information is available on the size, frequency and coincidence of different types of PSA activities).

However, the Commission has not attempted to quantitatively estimate or project PSAs' future mobile broadband requirements. Such an exercise is unlikely to yield robust results given extensive data requirements and the many unknown factors that will bear on demand, including:

- the availability of other communications systems (including LMR, WiFi and satellite)
- the pricing model and prices that PSAs face for mobile broadband services
- adjustments to PSA operational and communication procedures and protocols
- developments in mobile broadband technology (and applications), and the expansion of LTE networks.

Moreover, estimating PSAs' future demand for mobile network capacity was not considered feasible or worthwhile by the majority of study participants (box 4.7).

Box 4.7 Participant views on estimating demand

The accurate prediction of future data capacity requirements has proven to be extremely difficult and unreliable, both in the public safety and consumer mobile broadband environment. (Victorian Government, sub. 28, p. 29)

PSA's are still not experienced enough with the potential usage of mobile data to be able to accurately forecast their ultimate demands. (ARCIA, sub. 2, p. 3, 12)

It will be difficult to predict future demand requirements with a high degree of precision in this fast-moving environment. (Victoria Police, sub. 17, p. 13)

In general, it has proved extremely difficult to estimate what the upper limits of peak demands might be, given that the scale of events varies so greatly … It is likely that once PSMB becomes a reality, there will be latent demand emerging across the emergency services sector which cannot be predicted to any degree of accuracy at this stage. (MFB, sub. 6, p. 15)

Estimating PSA demand for mobile broadband is difficult for two reasons. First, there is uncertainty about how and for what applications PSA use of mobile broadband will develop over time. Second the unpredictable nature and location of events that PSAs are required to deal with. (Telstra, sub. 19, p. 31)

Actual demand for mobile broadband traffic often exceeds demand forecasts due to the introduction of new applications and services that were simply not anticipated by operators. (Ericsson, sub. 10, p. 15)

In any case, estimating PSAs' future demand for network capacity is not a critical requirement for this study. The Commission's task is focused on identifying the best way to deliver PSMB, irrespective of the level of capacity that the capability provides or how it changes over time.

PSAs are seeking a standard of service that would support data use in mission critical situations

The evidence submitted throughout this study suggests that the defining feature of a PSMB capability (relative to commercial mobile carrier offerings) is that it enables PSAs to use and rely on mobile broadband *data* services in mission critical situations. (As discussed in chapter 5, there are technical barriers to delivering mission critical *voice* services over LTE at the present time.)

However, participants provided little detail about the specific levels of service that are sought, or the way in which some of the quality characteristics important to PSAs (such as security or 'guaranteed' network access) should be met. That said, a broad consensus did emerge with respect to a number of quality characteristics, as outlined below. This provides some guidance on the quality features that are most important to PSAs and how these should be specified as part of a PSMB capability.

Participant views on a mission critical data network

Coverage

A number of participants considered that a PSMB capability should provide the same geographic and population coverage as LMR voice networks. For example, Motorola (sub. 12, p. 16) noted that:

> For PSMB to be fully Mission Critical it will require similar network coverage levels to narrowband networks. … Currently, PSA narrowband voice systems typically require 95-98% area coverage and often include in-building coverage.

The MFB (sub. 6, p. 11) pointed to the importance of 'in building' and rural coverage in particular.

> For the MFB, this includes in-building coverage, additional coverage in buildings via distributed antenna systems, so that portable hand held devices can be used throughout the coverage areas. Since the 2009 Black Saturday fires the MFB is increasingly responding to rural areas across Victoria, and responses interstate. In these circumstances we respond under the management of other agencies. In these cases we would expect to get the coverage those services get and interconnect with the services we are responding with.

The Victorian Government (sub. 28, pp. 24–25) highlighted that its LMR voice networks provide:

> coverage for vehicle-mounted terminals to approximately 96% of the State's geographic area, as well as up to 30 km out to sea, and overlapping coverage into neighbouring states. These networks cover close to 100% of the State's population, and have been designed to cover all major roads and railways, and a significant proportion of the State's bushfire-prone areas. In addition to the voice networks, the State also maintains a pager network for the dispatching of volunteers. This network covers approximately 97% of the State's geographic area.

However, while the Victorian Government (sub. 28, p. 25) considered that there is a 'business requirement' for radio and voice networks to provide 100 per cent geographic coverage, it recognised that 'fully meeting this requirement will never be feasible, so a risk-based analysis must be undertaken to direct coverage augmentation investments appropriately'.

Reliability (or resilience)

Participants generally considered that a PSMB capability should exhibit a higher level of reliability than commercial mobile networks currently provide. However, precisely what the desired standard is was not detailed in submissions and limited information is available publicly.

LMR voice networks are typically designed to deliver very high levels of network availability (a common measure of reliability). For example, the ACT Government (sub. 25, p. 4) noted that:

> Mission critical systems within the ACT Emergency Services typically operate on 99.999 per cent uptime. This very high availability level is indicative of the trust and requirement that is placed upon these systems.

Some participants considered that a PSMB capability should provide a comparable or better level of reliability to LMR networks, particularly if PSMB is to be the primary communications network for PSAs (VHA, sub. 11). However, other participants suggested that a lower level of reliability might be acceptable and/or more realistic. For example, the MFB (sub. 6) suggested that the different nature of LTE and LMR networks makes it difficult to directly compare reliability levels. PSMB reliability requirements might also be lower if there are 'layers' of communication and redundancy available (for example, if existing LMR networks continue operating), such that PSAs are not relying on PSMB *exclusively* (Victorian Government, sub. 28).

Interoperability, security and priority

There was strong support among study participants for a PSMB capability that facilitates inter-agency and inter-jurisdiction interoperability, user prioritisation and secure communication services. For example, the NSW Telco Authority (sub. 30, p. 47) considered that:

> Communications concerning criminal investigations, covert surveillance and national security operations must be secure. Security in this context does not just mean that communications cannot be intercepted and interfered with, but also that other information such as the location of handsets and devices is not available to non-authorised personnel, nor the meta data generated by and from these devices.

That said, participants provided little guidance as to how these outcomes should be achieved, or what meeting these objectives would mean for the PSMB delivery option. Moreover, participants appear to place different levels of importance on the achievement of these characteristics. For example, Motorola (sub. 12, p. 21) submitted that end-to-end encryption of communications, with no opportunity for interception in between, is fundamental to achieving security objectives.

> 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.

However, encryption (and security more generally) was not considered to be a high priority for all PSAs. Victoria Police (sub. 17, p. 14) observed that:

> The end-to-end information security requirements will differ amongst the PSAs because of the different missions of each PSA. For example, the CFA [Country Fire Authority] does not require its voice communications to be encrypted because it encourages its volunteers and interested community members to access its communications via scanners and web pages.

Other evidence on what constitutes a mission critical data network

As noted earlier, a number of other countries are contemplating or implementing a PSMB capability in various guises. Preparatory work undertaken in these countries reveals insights (albeit limited) about the service standards being pursued.

For example, the Statement of Objectives for the FirstNet project in the United States details that the PSMB capability should:

- achieve annual end-to-end availability of 99.9 per cent (up to 9 hours down time per year)
- support the static and dynamic prioritisation of public safety officers based on predefined user profiles (including the ability to change user profiles in real time in response to incidents). (FirstNet 2015d)

While information about the quality of service to be delivered over the UK Emergency Services Network is not publicly available, official sources suggest that the new network needs to provide end-to-end security (Shipley 2015) and a high level of coverage (98 per cent by population on an in-building basis and 90 per cent geographic coverage) (UK Home Office 2015b).

A 2010 report for the TETRA Association proposed a number of operational requirements that it considered essential to public safety communications in the United Kingdom, namely:

- annual end-to-end availability of 99.98 per cent (up to 2 hours down time per year)
- 80-bit end-to-end encryption of communications
- network coverage consistent with the typical organisational boundaries of PSAs, specifically, population coverage of 99.5 per cent for outdoor, 65 per cent for indoor, and 99.9 per cent for air to ground. (Analysys Mason 2010)

Many of these proposals were supported by a more recent report prepared for the European Commission (SCF Associates 2014). This report considered that a public safety network should have the same or greater resilience as the Airwave network (the narrowband data network in the United Kingdom), the provision of public safety features for data and voice (such as group call, push-to-talk and direct-mode communications), and priority of emergency services officers over commercial customers on the network.

There is no ‘one size fits all’ PSMB capability

In practice, the capacity and quality of a PSMB capability could take a range of values. However, delivering a PSMB capability has costs, and many of these costs (met by governments and ultimately taxpayers) are likely to increase exponentially with capacity and service standards (box 4.8).

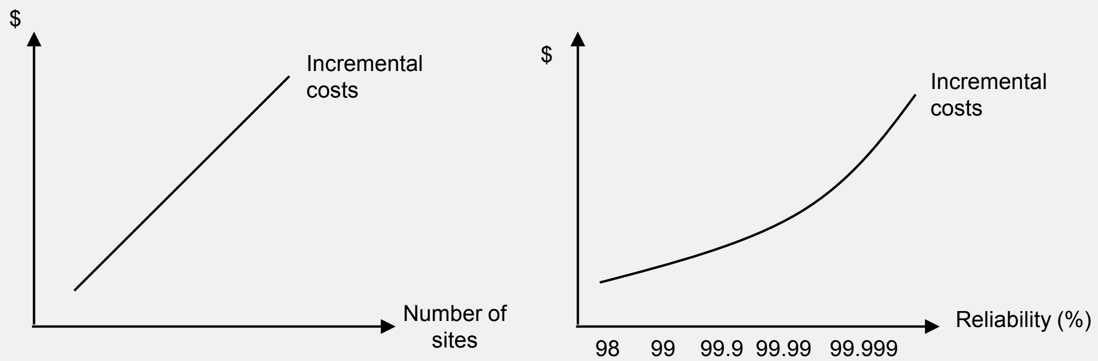
It is in the best interests of the community for individual jurisdictions to pursue a capability that reflects their particular needs and circumstances and their communities' willingness to pay for public safety grade mobile broadband services. A uniform capability across all jurisdictions is unlikely to be efficient. Dramatic differences in population densities (and the likelihood and materiality of emergencies) across different regions means that a variable capability *within* jurisdictions is also likely to be warranted, especially with regard to network capacity.

That said, the considerable uncertainty about how PSAs will use mobile broadband applications, and about the benefits of that use, is a reality for all jurisdictions. It is prudent, therefore, for all jurisdictions to 'start small' in rolling out a PSMB capability, irrespective of the deployment approach chosen. This could mean commencing with a modest level of network capacity and service quality, but with scope to scale up capacity and quality standards over time, as PSAs gain experience with mobile applications and the business case develops. This approach would also ensure that PSAs have sufficient time to make the operational changes necessary to get the most out of PSMB. These issues are discussed further in chapter 7.

Box 4.8 **Greater reliability comes at an increasing cost**

Evidence presented to this study suggests that a PSMB capability would need to deliver very high levels of network reliability — measured as the portion of time the network is available — to support the use of mobile data applications in mission critical situations. Reliability levels in the order of 99.9 to 99.999 per cent have been canvassed (equivalent to annual down time of about 9 hours or 5 minutes respectively).

However, achieving high levels of network reliability has costs, and greater levels of reliability tend to come at an increasing cost (see figure). Reliability is a function of the number of mobile sites that need to be hardened and the extent of hardening required at each site. As reliability levels increase (say from 98 per cent to 99 per cent), proportionally more hardening (investment) is required to deliver the same unit increase in reliability standards. This reflects the increasing severity of risks that need to be mitigated to reach higher levels of reliability.



4.4 PSMB scenarios for analytical purposes

The Commission has undertaken a quantitative analysis to better understand how the costs of delivering a PSMB capability vary depending on the delivery option (chapter 6). A necessary part of this analysis is to require that the same level of PSMB capability is delivered under each option, such that they are evaluated on an even keel as far as possible.

To this end, the Commission has specified a number of PSMB ‘scenarios’ that define a specific level of capacity to be delivered over the planning horizon. **Importantly, these scenarios are not suggestive of the type of capability jurisdictions should adopt, or of PSA demand for mobile broadband.** Rather, using these scenarios in the quantitative cost analysis has enabled the Commission to:

- examine how the costs of delivering a given PSMB capability vary across delivery options
- consider whether (and, if so, how) the relative cost effectiveness of alternative delivery options changes depending on the amount of capacity that is delivered.

Capacity

The capacity metric used in the Commission’s quantitative analysis is the total amount of capacity available to PSA users at a given location and time (that is, Mbps/km^2). This approach was supported by a number of study participants — for example, the Victorian Government (sub. 28, p. 30) considered that ‘the best metric to define and/or measure service capacity is uplink bits per second (bps) within a specific area (km^2)’.

Three levels of network capacity have been considered

In the central (or base) case, it is assumed that the PSMB capability would provide end users in dense urban areas with network capacity of 1.5 Mbps/km^2 (uplink and downlink). This compares to capacity levels of about 10–100 kbps for LMR data networks (chapter 2).

In practice, it is likely that PSAs’ demand for uplink capacity will exceed downlink demand (section 4.1). However, even though preferences for uplink and downlink capacity may be asymmetric, the nature of mobile networks is such that they are typically dimensioned to meet the greater of the two.

Network capacity of 1.5 Mbps/km^2 would be sufficient to support the simultaneous use of two to three mobile devices running real-time video-based applications at any given time, in every square kilometre (assuming each video requires capacity of 500 to 1000 kbps (Adobe nd)). Other mobile applications have far lower capacity requirements — accordingly, 1.5 Mbps/km^2 would also support the simultaneous use of one mobile device running a video application and at least 20 devices conducting database checks, sending emails and tracking the location of vehicles (assuming each device would require about 50 kbps (CSS 2011)) .

A higher and lower level of capacity have also been considered to understand the sensitivity of the quantitative results to different levels of demand (chapter 6).

- The upper bound estimate of 4.0 Mbps/km^2 would support the simultaneous use of at least 4 and as many as 8 video-based applications in every square kilometre of dense urban areas.
- The lower bound estimate of 1.0 Mbps/km^2 would be sufficient for about 1 to 2 videos, or 20 devices accessing lower-capacity applications, in every square kilometre of dense urban areas.

In each case, a lower amount of network capacity is provided in less densely populated regions, as described in table 4.1.

In developing these scenarios, the Commission has considered:

- the demand figures cited by the Victorian Government (box 4.5)
- the network capacity levels associated with the FirstNet project in the United States, and the incident scenario work undertaken in Canada in 2011 (section 4.3)
- confidential information provided to the Commission on PSAs' current data usage over commercial carrier networks.

The Commission has also had regard to the network capacity assumptions detailed by the NSW Telco Authority (sub. 30). The Authority suggested that a PSMB capability should provide a theoretical maximum data speed of 10 Mbps. The Commission's scenarios are described in terms of *average* data speeds (such as 1.5 Mbps/km^2 in the central case). However, a user standing right next to a mobile tower would receive much higher speeds (possibly up to 10 Mbps) than average. The Commission's quantitative analysis is based on the same cell edge data rate cited by the NSW Telco Authority (256 kbps).

Table 4.1 **PSMB scenarios**

	Central case	*Lower bound*	*Upper bound*
Dense urban, urban and suburban areas			
PSMB capacity	1.5 Mbps/km^2	1 Mbps/km^2	4 Mbps/km^2
Growth rate	5% pa	2% pa	10% pa
Rural and remote areas			
PSMB capacity	500 kbps/km^2	200 kbps/km^2	800 kbps/km^2
Growth rate	5% pa	2% pa	10% pa

Growth rates

The Commission's quantitative cost analysis covers a 20-year horizon and is based on meeting PSA capacity requirements (as defined by the above scenarios) each year.

To project capacity levels over this period, the Commission has applied a growth rate of 5 per cent per annum in the central case. Sensitivity testing has been conducted to consider the implications of lower and higher growth rates (2 and 10 per cent per annum respectively).

As discussed in chapter 3, mobile broadband usage in Australia (by the general public) is growing at a rapid rate and this is projected to continue. For example, some estimates suggest that mobile broadband data traffic in Australia is expected to increase by 38 per cent each year between 2013 and 2017 (CIE 2014).

In this context, the growth rates built into the Commission's PSMB scenarios may appear modest. However, it is important to understand that commonly reported mobile broadband growth rates tend to focus on *stock* rather than *flow* measures (box 4.1). Stock measures capture how the total volume of data consumed in a given period (such as GB per year) changes over time. These measures tend to exhibit much higher rates of growth than measures focused on data usage (or demand) at a given point in time (such as Mbps). This reflects the fact that a lot of the growth in mobile broadband traffic volumes is due to people using their mobile devices more frequently and more customers taking up mobile devices.

Applying aggressive growth rates to the network capacity metric used here (Mbps/km^2) risks overstating the amount of capacity that PSAs would need (or could feasibly use) at a given location and point in time. For example, a 38 per cent annual growth rate applied to the central case would mean that PSAs have access to over 900 Mbps/km^2 in year 20 — it is highly unlikely that such extensive mobile device usage would be efficient during most plausible emergency incidents. By contrast, under the central case assumptions (1.5 Mbps/km^2 in year 1, increasing at 5 per cent per annum) the PSMB capability would provide PSAs with 4.0 Mbps/km^2 in year 20 (or 27 Mbps/km^2 using the upper bound assumptions of 4.0 Mbps/km^2 in year 1, increasing at 10 per cent per annum).

Service quality

The key distinguishing feature of PSMB — from a service quality perspective — is that it can be relied upon in mission critical situations.

The Commission has attempted to identify a set of mobile broadband quality standards that fit this brief, namely:

- 99.9 per cent end-to-end availability (up to 9 hours down time per year)
- preferential (priority) services to PSAs that can be adjusted dynamically

- interoperability across PSAs and jurisdictions
- population coverage of at least 99 per cent
- secure communications which are end-to-end encrypted.

However, in light of the limited and inconsistent evidence available on mission critical data standards, the Commission expects that these standards will be revised ahead of the final report, subject to receiving feedback.

For some of these standards, there has also been limited and conflicting evidence relating to whether and what technologies could be put in place to achieve those outcomes. As a result, the options analysed in chapter 6 are not explicitly designed to meet all of these standards.

Nevertheless, certain levels of service quality are implied by the assumptions made in the quantitative analysis. Under each delivery option evaluated:

- the network has been designed to provide geographical coverage equal to existing commercial networks, which equates to a population coverage in excess of 99 per cent
- some capital investment is made to provide preferential or priority services to PSAs
- it is assumed that a proportion of network sites are subject to some form of hardening — including the installation of additional battery backup and civil upgrades — which implies some improvement to network resilience and reliability.

The Commission's approach to the quantitative analysis is discussed further in appendix C.

DRAFT FINDING 4.3

PSAs expect a PSMB capability to deliver a standard of service that would allow them to use mobile broadband data applications in 'mission critical' situations (where there is a material risk of loss of life or severe injury).

However, operationalising the concept of a mission critical data network is difficult. The Commission has proposed a starting point definition for service quality. Specifically:

- the network should be available 99.9 per cent of the time, and cover at least 99 per cent of the population
- PSAs should be provided with priority access to (and capacity on) PSMB networks, with scope to change these arrangements in real time
- PSAs should be able to communicate with each other (within and across jurisdictions), including by accessing PSMB networks upon crossing jurisdictional borders
- communications over a PSMB network should be secure.

INFORMATION REQUEST

The Commission is seeking feedback on how it has operationalised the concept of a mission critical mobile broadband data network (draft finding 4.3).

5 How can a PSMB capability be delivered?

Key points

- A 'public safety grade' mobile broadband (PSMB) capability could be delivered through a dedicated network, a commercial approach, or various hybrids.
- There is broad consensus that a PSMB capability should be delivered using Long Term Evolution technology (LTE) — it has various enhancements over previous mobile technologies, and will continue to evolve and improve.
- Key drivers of the cost of delivering a PSMB capability are the network coverage and capacity requirements, which are met using a mix of infrastructure and spectrum.
  - Infrastructure requirements include mobile sites and equipment, transmission backhaul and central network systems.
  - Spectrum has opportunity costs — the foregone alternative uses of that spectrum — that need to be considered alongside the costs of other inputs.
- Commercial mobile network operators have existing networks which cover most of the population, and hold large parcels of spectrum.
- Meeting public safety agencies' (PSAs) requirements for PSMB poses technical, economic and commercial challenges under any approach. However, it is technically feasible to deliver this capability under a dedicated, commercial or hybrid approach.
- Commercial approaches (and to a lesser extent, hybrid approaches) avoid many of the upfront infrastructure costs required under a dedicated approach, and can take greater advantage of ongoing operating efficiencies. However, costs are not the whole story — there are differences in risks between approaches (chapter 6).
- Irrespective of the approach to delivering PSMB, costs can be minimised by leveraging existing infrastructure where feasible, sharing network capacity among PSAs on an efficient basis and allowing for flexible use of spectrum across users.
- Flexibility in delivery will help to minimise costs and deliver a sustainable PSMB capability. This can be facilitated by relying on common technical standards, and focusing initially on a PSMB data capability (given that key technical questions need to be resolved before 'mission critical' voice services can be delivered over PSMB). Existing land mobile radio networks are likely to remain in place for the foreseeable future for the delivery of mission critical voice.
- Extending a permanent PSMB network beyond the footprint of commercial networks on a large geographic scale would be costly under any approach. Deployable mobile cells or use of alternative technologies, such as satellite broadband, offer a more cost-effective option in some parts of Australia.

The key requirements of a Public Safety Mobile Broadband (PSMB) capability (chapter 4) could be met in several ways. This chapter looks at the technical considerations and cost drivers on the supply side. It steps through considerations relating to: network capacity and coverage; preferential access; roaming; network reliability; interoperability and security; and timing and sustainability. The focus is on how these factors might vary depending on the delivery approach, setting the scene for the evaluation of costs, benefits and risks of specific options in chapter 6. Issues relating to implementation — including institutional arrangements and contracting — are discussed in chapter 7.

5.1 Delivery approaches for PSMB

The terms of reference refer to three high-level approaches for delivering PSMB — a dedicated PSMB network, an approach fully reliant on commercial networks, or a combination of the two (hereon 'hybrid' approach). Study participants (hereon 'participants') offered views on what these approaches might look like (box 5.1). The essential elements of each are described below.

A dedicated PSMB network

At the most basic level, a dedicated PSMB capability would mean public safety agencies (PSAs) have access to (and control over) their own mobile broadband network which is constructed and operated to a given set of standards (hereon a 'dedicated network'). To minimise capital deployment costs, a dedicated approach would likely involve leveraging existing network infrastructure (such as mobile sites and backhaul transmission (section 5.2)) owned by PSAs, state and territory governments (hereon 'states') and commercial mobile carriers (hereon 'mobile carriers'). Importantly, a dedicated network for PSMB would require its own dedicated radiofrequency spectrum.

A commercial approach

A commercial approach would mean that PSAs obtain PSMB services from one or more of the mobile carriers through a contract for service. Providers would determine how best to meet PSA requirements using their own mobile networks and spectrum holdings. This approach would not involve any dedicated spectrum for PSAs, but would require mobile carriers to adapt their networks to meet the higher quality requirements implicit in a PSMB capability.

Hybrid approaches

A hybrid approach would involve elements of both the dedicated and commercial approaches. There are various forms a hybrid could take.

For example:

- constructing and operating a dedicated PSMB network for a targeted coverage area (with dedicated PSMB spectrum), and using mobile carrier networks and other options (such as deployable cells) elsewhere
- integrating PSMB spectrum into an existing mobile carrier's network, such that PSAs have a 'dedicated lane' on the network and the ability to overflow to a commercial mobile carrier (or carriers') network as required.

Depending on the specific design, a hybrid approach could fall closer to a dedicated PSMB network or a commercial approach (SCF Associates 2014). Several hybrids are evaluated in chapter 6.

Box 5.1 Participant definitions of PSMB delivery approaches

Dedicated approach

Telstra understands a dedicated network relates to either: A fully private network with no carrier elements utilised in the delivery of the PSMB capability; or A privately built network that does not utilise a commercial network service provider mobile broadband core but does uses (sic) other commercial network facilities, infrastructure and/or backhaul services via commercial arrangements, as is currently the case currently in certain jurisdictions for the provision of LMR. (Telstra, sub. 19, p. 7)

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. (Motorola, sub. 12, p. 24)

Commercial (or carrier) approach

A carrier model is similar to a carrier hybrid model except no dedicated capacity (including spectrum) is made available. The PSMB data is prioritised and carried on the shared carrier's network capacity. (Telstra, sub. 19, p. 7)

Hybrid approach

Where commercial carrier coverage exists, it is proposed that their capacity be virtualised, hardened and partitioned and that a PSMB be virtually delivered by collocating and sharing existing sites, power, towers and backhaul. (BAI, sub. 1, p. 5)

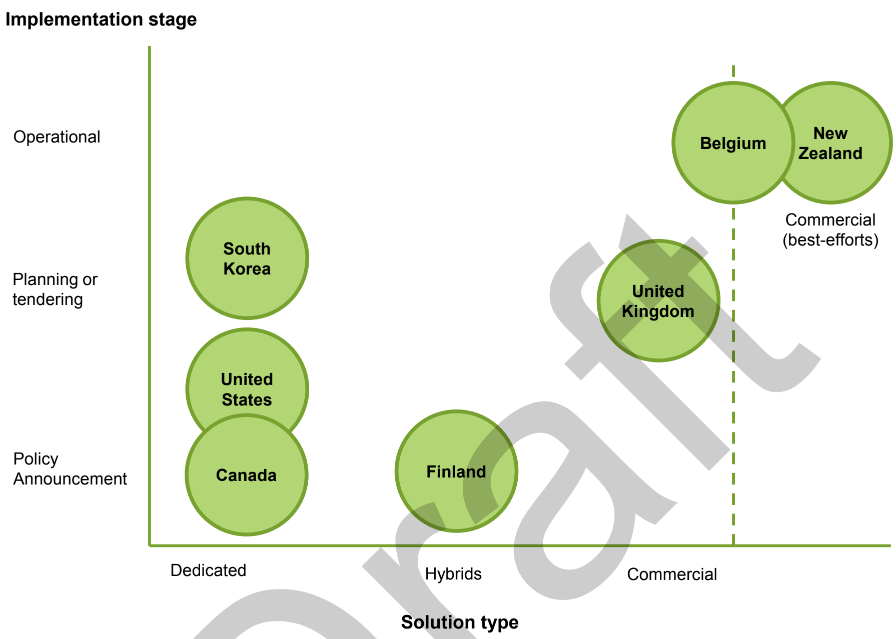
Telstra considers there are two hybrid variations that are relevant for consideration: A private dedicated PSMB capability that can roam onto a public carrier network. [or] Carrier provision of some dedicated PSMB capacity and seamless overflow to the carrier's public network (e.g. Telstra LANES™ model) where the PSMB traffic is given priority. (Telstra, sub. 19, p. 7)

An alternative, less infrastructure dependent approach to delivering a PSMB services (sic) is for PSAs to pursue a service provider model underpinned by agreements with multiple MNOs on a 'pay-per-use' basis. This solution could be implemented via agreements with two or three MNOs. (VHA, sub. 11, p. 7)

… [T]here are numerous variations for a hybrid model. It is likely that a hybrid model will ultimately be deployed in Australia, gaining the best aspects of existing MNO and public safety agency infrastructure, and balancing the needs of higher population densities in the cities and larger town centres against the low density population and lower demand anticipated in rural and remote areas. (NSW Telco Authority, sub. 30, p. 27)

There are various approaches to PSMB being investigated, planned or implemented in other countries which lie somewhere on the continuum between a dedicated and a commercial approach. Some countries are more advanced than others (figure 5.1). Appendix B provides further information on international developments.

Figure 5.1 **Diverse international approaches to PSMB**



5.2 Understanding mobile networks

Delivering a PSMB capability involves designing and implementing a mobile broadband network to meet a given level of capability (chapter 4). Doing so raises a series of decisions about which inputs to use, and the extent to which existing infrastructure and other resources can be leveraged (or shared) to deliver it cost effectively.

A mobile network has four key elements

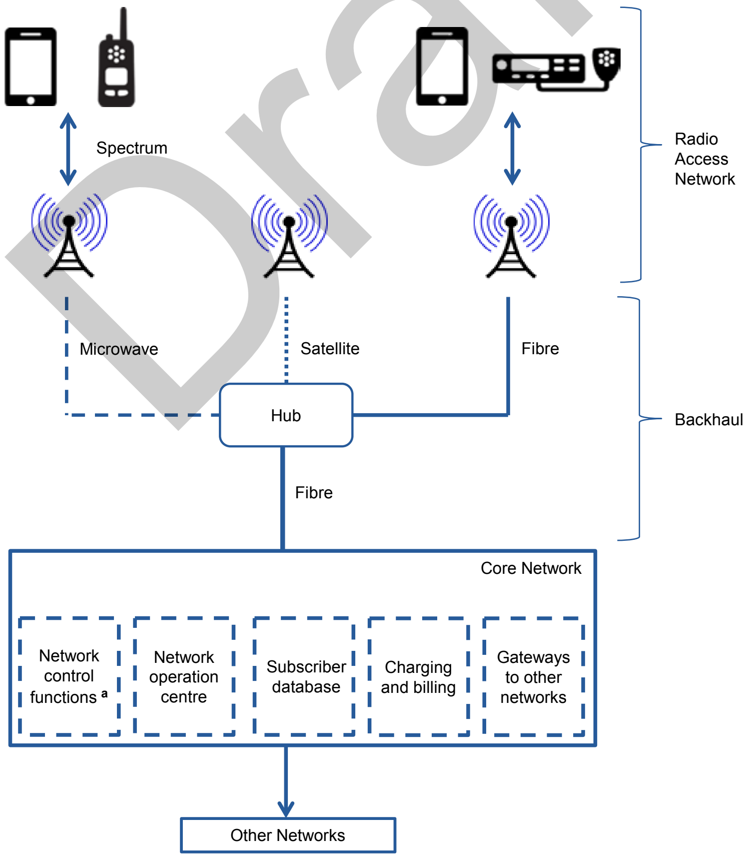
Mobile networks are highly capital intensive. They involve large fixed costs upfront to deploy the network, significant ongoing operating expenditure to operate and maintain it, and recurring investment to continually upgrade it.

Broadly, a mobile network consists of four elements (figure 5.2).

- Radio access network — a large number of mobile base station sites (heron 'sites') containing equipment such as radio antennas, a transmission tower, hardware and software. Each mobile cell (hereon 'cell') can only transmit and receive information over a limited range, and is defined by its size, coverage range and capacity potential.

- Backhaul transmission (hereon 'backhaul') — the high capacity links carry large volumes of data from sites back to the core network — either underground (using optical fibre links) or in the air (using microwave or satellite technology). Some elements of mobile backhaul networks are designed in a 'ring', 'mesh' or 'tree pattern' to ensure there are multiple ways in which data traffic can be routed (ACCC 2014a; Nadiv and Naveh 2010).
- Core network — the 'brains' of the network. It is a collection of elements that together control and manage the network). Typically a mobile network would have one core network with redundancy to avoid a single point of failure.
- Radiofrequency spectrum — a natural resource that can be used in the transmission of information via electromagnetic waves. These waves can be transmitted at a range of different frequencies.

Figure 5.2 **Key elements of a mobile network**



a 'Network control functions' refers to the variety of functions that different elements of the core undertake when managing a call or data session on a mobile network, such as user authentication, assigning resources, traffic management, and cell handover.

Sources: Alcatel-Lucent (2009, 2010); Gras (2015).

All of the inputs above involve costs. Some, such as the costs of deploying network equipment and infrastructure, are highly visible and have clear financial implications. Other inputs, particularly spectrum, are less tangible but still involve opportunity costs (box 5.2).

Box 5.2 Spectrum has opportunity costs

Spectrum is a limited resource. To minimise interference with other users and ensure spectrum allocation meets various policy objectives, the Australian Communications and Media Authority regulates the use of spectrum. The main objectives of Australia's regulatory framework are to allocate spectrum to its most efficient use and to make adequate provision for public and community services.

An essential consideration in allocating spectrum is its opportunity cost — the value of the next best alternative use that is forgone when spectrum is allocated to a particular use or user.

Several factors influence the potential uses of spectrum, and hence its opportunity cost:

- the frequency — spectrum in lower bands has greater propagation (coverage), whereas higher bands offer greater throughput due to the increased bandwidths available
- international harmonisation — bands are typically of greater value to mobile carriers when they are supported by international manufacturers of network equipment and end-user devices
- the bandwidth — the amount of spectrum available
- location — other things equal, demand for mobile broadband spectrum is likely to be higher in metropolitan areas where there are more people (and more need to add to capacity), and lower in regional areas where traffic demand is lower.

The opportunity cost of spectrum is likely to increase as consumers make greater use of smartphones, tablets and other data-intensive devices into the future.

Sources: Department of Communications (2015b); OECD (2014).

Spectrum is a key input for PSMB

The type and amount of spectrum used in a mobile network has an important bearing on how networks are designed — principally because it influences how many sites are needed to deliver a given level of capability.

Different types of spectrum have different technical properties. Generally speaking, lower frequencies provide a wider coverage range (and better penetration of buildings), whereas larger bandwidths are available at higher frequencies, thereby allowing higher capacity to be provided within a cell. Spectrum frequencies under 1 GHz are considered highly desirable for mobile broadband, although mobile operators typically have a mix of spectrum types for different purposes and geographic areas (table 5.1). The cellular nature of mobile networks means spectrum is reused in adjacent cells, thereby allowing a large geographic area to be covered with only a limited set of frequencies.

Table 5.1 Australian mobile carrier spectrum holdings

Band	*Optus*	*Telstra*	*Vodafone Hutchison Australia*
700 MHz	2 x 10 MHz national	2 x 20 MHz national	..
800 MHz	..	2 x 10 MHz national 2 x 5 MHz outside five largest cities	2 x 10 MHz five largest cities 2 x 5 MHz in Canberra, Darwin, and Hobart
900 MHz	2 x 8.4 MHz national	2 x 8.4 MHz national	2 x 8.2 MHz national
1800 MHz	2 x 15 MHz in largest five cities Small number of regional licences	2 x 20 MHz in Adelaide, Brisbane and Perth 2 x 15 MHz in Melbourne and Sydney 2 x 10 MHz in Canberra, Cairns and Hobart 2 x 12.5 MHz to 2 x 15 MHz regional areas	2 x 30 MHz in Melbourne and Sydney 2 x 25 MHz in Adelaide, Brisbane and Perth 2 x 5 MHz in Canberra, Darwin and Hobart
2 GHz	2 x 20 MHz metro 2 x 15 MHz regional 2 x 10 MHz remote	2 x 15 MHz metro 2 x 20 MHz regional 2 x 10 MHz remote	2 x 25 MHz in Melbourne and Sydney 2 x 20 MHz in Adelaide, Brisbane and Perth 2 x 10 MHz in Canberra and Darwin 2 x 5 MHz in regional areas
2.3 GHz	98 MHz in Adelaide, Brisbane and Perth 91 MHz in Melbourne and Sydney 70 MHz in Canberra	..	..
2.5 GHz	2 x 20 MHz national	2 x 40 MHz national	..

Sources: ACMA (2015e); Analysys Mason (2015); CIE (2014).

Another key component of providing users with mobile broadband capability is end-user devices. End users communicate over a mobile network using different types of portable devices to send and receive information — such as smartphones, tablets and vehicle-mounted terminals. To access the network, a device must have computer chips and software compatible with the spectrum band(s) being used on the network. Users can usually cross into different cells without losing connection.

Network sharing already occurs in the mobile sector

As a means of minimising capital and operating costs, mobile carriers often share radio access network infrastructure through commercial negotiation — carriers also have regulatory obligations to provide access to third parties under certain circumstances (chapter 7). Typically, this involves mobile carriers sharing passive infrastructure, such as physical sites, towers and power supplies.

More extensive forms of sharing involve mobile carriers sharing equipment, such as spectrum and base station equipment (Alcatel-Lucent 2010; GSMA 2012; Mahindra et al. 2013; NEC 2013), and this capability is supported by recent Long Term Evolution (LTE) technical standards (ATF, sub. 4, attachment. 5). Apart from the roaming arrangements between Optus and VHA in selected regional areas, it appears that active radio access network sharing is less prevalent in Australia than in some international markets (Coleago Consulting 2015).

LTE differs from previous generation mobile technologies

Mobile technology continues to evolve. The latest generation technology is LTE, a fourth generation (4G) technology. LTE technology is based on open international standards set by the 3rd Generation Partnership Project (3GPP) and are periodically updated on a regular 18-24 month cycle (ATF, sub. 4, attachment 3). LTE has various enhancements compared with previous generation mobile technologies, and technical standards for the public safety sector are currently in development (box 5.3).

LTE is the accepted technology for PSMB

There is widespread agreement — both internationally and amongst participants — that PSMB should be delivered using LTE technology regardless of the delivery approach. The 3GPP LTE standard has been endorsed nationally, regionally, and internationally as a preferred technology standard to support commercial and mobile broadband networks for 'Public Protection and Disaster Relief' (appendix B).

Box 5.3 LTE technical standards

Features already in the LTE standards

Based on the technical standards already in place (Release 12 was finalised in March 2015), LTE has various enhancements over previous generation mobile technologies, including:

- it provides higher peak data rates
- it facilitates greater use of 'small cells' which can allow spectrum to be used more efficiently
- traffic at the edge of a cell can be more effectively shared by multiple adjacent cells, which takes the pressure off any one cell
- the ability to apply differentiated Quality of Service, priority and pre-emption mechanisms for different users and applications
- the ability to use 'carrier aggregation' which enables mobile carriers to mix and match (non-contiguous) combinations of spectrum into a virtual single block in order to scale up capacity for a specific group of users or applications in an individual area when needed
- the ability for automatic detection and removal of failures, and automatic configuration of networks
- the ability to use device-to-device communications to enable direct-mode communication between proximate users even when the network is unavailable.

Standards under development for the public safety sector

Future releases are focusing on the development of mission critical voice applications over LTE, and a specific 3GPP working group has been set up for this purpose.

- Release 13 is expected to be finalised in March 2016. Aside from various other enhancements, it will include technical standards to facilitate the delivery of mission critical voice applications over LTE — including push to talk and group-calling capability.
- Release 14 is expected to be finalised around mid-2018 and is expected to include mission critical video. Releases 14 and 15 could become the beginnings of fifth generation (5G) mobile technology.

Sources: 3GPP (2015b, 2015d, 2015e); 4G Americas (2013); ACMA (sub. 14; 2013d); Ericsson (sub. 10); P3 Communications and TCCA (2015).

5.3 Coverage and capacity requirements

The design of a mobile network is driven largely by the desired level of coverage and capacity. These considerations are inter-related (Motorola, sub. 12). Typically, the design or 'dimensioning' of a mobile network first involves establishing a coverage layer (coverage sites), then adding additional sites for capacity in specific areas to meet expected demand (capacity sites). The higher the defined level of 'quality' attached to the coverage layer (indoor, in-tunnel, outdoor handheld or in-vehicle) the more capacity is provided to users as a minimum standard (Telstra, sub. 19).

There are potentially significant differences in how capacity and coverage would be provided under different PSMB delivery approaches, and the costs involved.

Coverage and capacity are key drivers of network costs

A very high proportion of the capital and operating costs of mobile networks are associated with providing and maintaining the coverage layer. A recent modelling exercise commissioned by the Australian Media and Communications Authority (ACMA) indicated that coverage is a more significant driver of the number of LTE sites in a network than capacity (Analysys Mason 2015).

There are technological limitations to how far mobile base station equipment can transmit over a geographic area. But other factors can also affect coverage. Coverage (and capacity) can differ depending on the end-user device — for example, vehicle-mounted antennae can pick up a signal further from a cell site than handsets can. It can also vary depending on whether a user is outdoors, indoors or underground. The quality of coverage required influences the density of the network, and the types of sites and spectrum used (chapter 6).

Adding capacity to a mobile network is also an important driver of costs. As such, in delivering a PSMB capability it is important to ensure that capacity is utilised as efficiently as possible. This means sharing capacity amongst PSAs on a flexible basis, rather than allocating a fixed amount to each individual agency (a ‘partitioned network’).

Mobile carrier networks have extensive population coverage

Coverage of mobile carrier networks in Australia is typically presented as a proportion of the population. Combined, commercial 3G and 4G networks cover around 98 to 99 per cent of the population (depending on the network), but significantly less in terms of Australia’s landmass (in the order of 5 to 30 per cent) — although these figures vary across states and mobile carriers (box 5.4). The coverage of commercial networks is often different to land mobile radio (LMR) networks, although the nature and extent of this difference varies across states and territories (chapter 2).

The coverage of mobile carrier networks is not static. The commercial case for extending and upgrading mobile carrier networks evolves over time with changes to technology, spectrum holdings, population movements and the pricing of complementary inputs (such as backhaul). Policy initiatives and funding programs by governments also have an impact, as do regulatory arrangements (chapter 7).

Box 5.4 **Mobile network coverage in Australia**

All three mobile carriers have high population coverage on their 3G networks.

- Telstra's 3G mobile network (NextG) covers 99.3 per cent of the population, equivalent to 2.36 million square kilometres on land (or around 31 per cent of Australia's landmass).
- Optus' 3G network covers 98.5 per cent of the population, equivalent to 1 million square kilometres (or around 13 per cent of Australia's landmass).
- VHA's 3G network covers 95.4 per cent of the population equivalent to around 350 000 square kilometres (or around 5 per cent of Australia's landmass), although VHA customers can roam on Optus' network in selected regional areas under a commercial agreement.

Each mobile carrier continues to expand its 4G network coverage, but at this stage it trails 3G coverage. For example, Telstra's 4G (LTE) coverage was expected to reach 94 per cent of the population by mid-2015, and it recently announced it would continue to extend its 4G footprint to 99 per cent of the population (and 2.5 million square kilometres) by 2017. Optus' 4G coverage is currently at 86 per cent of the population.

Sources: Analysys Mason (2015); Optus (sub. 18; 2012); Penn (2015); Telstra (sub. 19).

The costs of providing coverage and capacity differ across approaches

The costs of meeting PSMB coverage and capacity requirements are likely to vary substantially depending on whether a dedicated, commercial or hybrid delivery approach is pursued.

There are different ways to deliver network coverage and capacity

Three main factors determine the potential network capacity that can be provided by a mobile network.

- Spectrum — a larger amount of spectrum can deliver greater capacity, depending on its frequency.
- Network infrastructure — a larger number of overlapping cells can deliver greater capacity.
- Spectral efficiency — some technologies can carry a greater amount of data per MHz of spectrum than others (ACMA, sub. 14).

Dimensioning a mobile network requires translating measures of user capacity (or their data requirements) into network capacity measures that can be used for planning and design. Typically this requires the use of demand and traffic models — which provide the link between average usage, applications and total peak demand.

There are two key steps in dimensioning a mobile network.

- To dimension an initial coverage layer for a mobile network, a 'cell edge' data rate is typically used as the 'worst case' scenario from a technical perspective that a user could expect if operating the furthest away from a mobile tower (this measure does not take account of expected traffic in the cell).
- To take into account traffic demand, average demand per user could be estimated as a starting point, and then aggregated over all users to give a total demand per application or across a user group (during the busy hour) (chapter 4).

While all mobile networks need spectrum, there is a tradeoff between spectrum and infrastructure, assuming technology of a given spectral efficiency (ACMA, sub. 14). This means that, in some cases, it is possible to deliver the same level of capacity over less spectrum by building more infrastructure, or vice versa. This tradeoff is most relevant in areas where mobile networks are dense (such as metropolitan areas) — it does not work as well in less densely populated rural and remote areas because of technical and regulatory constraints on increasing cell size beyond a certain distance (such as those stemming from current regulations for the power of transmissions) (ACMA, sub. 14).

The spectral efficiency of technology influences the extent of the tradeoff between spectrum and sites. The shift to LTE technology has improved the level of capacity that can be provided by a given set of spectrum and infrastructure inputs (box 5.3).

Existing mobile carrier infrastructure may be more readily leveraged in a commercial approach

There is broad consensus across participants that leveraging the use of existing infrastructure, where feasible, would significantly lower the costs of delivering a PSMB capability and is a desirable objective irrespective of the approach taken (BAI, sub. 1; Optus, sub. 18; Telstra, sub. 19; Victorian Government, sub. 28). The potential to use or share existing infrastructure arises in various ways.

- Sharing existing mobile carrier cell sites — approximately 15 000 unique mobile carrier sites have already been deployed across Australia (ACMA 2015e).
- Leasing commercial backhaul capacity — there is a well-developed market for the provision of backhaul transmission capacity (particularly in metropolitan areas and major regional centres), over optical fibre, microwave and satellite technology (and existing carrier sites already have backhaul in place for their commercial operations).
- Governments leveraging publicly owned infrastructure — for example, the use of existing sites and backhaul capacity already deployed for operation of LMR networks, or sites and other infrastructure resources in the transportation, maritime communications or defence sectors. (While government's may pay a lower price for using their own sites than if carrier sites were used, this still has opportunity costs which would need to be considered in an evaluation of economic costs).

- Leveraging other complementary telecommunications network infrastructure — for example, seeking to access fibre, wireless or satellite capability deployed (or that will be deployed) as part of the NBN rollout.

In principle, it would be possible to leverage these network elements under all PSMB delivery approaches to the same extent, provided it is technically feasible, there is spare capacity, and appropriate commercial arrangements can be put in place within the current regulatory regime that governs these matters (chapter 7). That is, even under a dedicated approach, space could be sought on existing mobile carrier sites, or backhaul capacity could be leased from the commercial market, thereby considerably reducing infrastructure deployment costs compared to a 'greenfields' build.

As noted by the Australian Mobile Telecommunications Association (sub. 21, p. 2):

> Unnecessary duplication of infrastructure should be avoided. Industry members have well-established policies and processes in place to enable the sharing of physical infrastructure via the Mobile Carriers Forum (MCF) and similar commercial sharing arrangements should be considered in the design of any PSMB capability.

At face value the large number of existing mobile sites appears far in excess of what would be needed to meet the capacity and coverage requirements of a PSMB capability (at least in areas where mobile carriers have coverage). This suggests that the amount of new (or 'greenfields') sites that would need to be acquired and prepared for the installation of mobile infrastructure could be relatively limited.

However, leveraging existing commercial infrastructure on a large scale is not without challenges. While numerous, carrier sites will not necessarily have spare capacity that could easily accommodate new dedicated equipment for PSMB (particularly where mobile carriers reserve sufficient space for their future needs). Further issues which may constrain site sharing include ensuring that sites remain within tolerance levels for electromagnetic energy emissions, and do not violate any property restrictions.

Sharing mobile carrier infrastructure in the delivery of PSMB would be implicit in a commercial approach, and mobile carriers would have a strong incentive to do this in the most efficient way possible to minimise their total network costs. By contrast, in a dedicated approach (and some hybrid approaches), separate arrangements would need to be negotiated with mobile carriers on gaining access to existing infrastructure, such as sites.

Where it is not feasible to access mobile carrier sites, LMR sites could be leveraged and adapted to facilitate the delivery of a dedicated approach in order to minimise upfront deployment costs, as could state-owned backhaul capacity. The ability for states to leverage their own infrastructure to deploy a PSMB capability will vary across jurisdictions depending on the range and architecture of the LMR networks, or other relevant state-owned infrastructure.

An expected advantage of using LMR sites is that they may already be 'hardened' to standards considered acceptable for delivery of PSMB, in terms of power back-up and civil construction standards. On the other hand, LMR networks typically have many fewer sites than mobile carrier networks and may not be sufficient for deploying a PSMB capability (for example, in Victoria there are approximately 200 unique sites across the StateNet and Rural Mobile Radio networks, compared to over 3800 unique mobile carrier sites) (ACMA 2015e; Nally 2014).

This suggests that, where it is not possible to share use of mobile carrier sites for delivering a PSMB capability, a dedicated approach would likely require some newly constructed sites.

A dedicated approach requires the installation of new equipment upfront

A dedicated approach to PSMB would involve constructing a coverage layer across the targeted network coverage footprint. Even where an existing site can be leveraged to avoid a greenfields build (discussed above), significant costs would be incurred, including:

- the deployment of new mobile base station equipment in each cell (to operationalise the dedicated spectrum)
- purchasing (or where not possible deploying new) backhaul capacity to service each site (unless an LMR site already had sufficient backhaul capacity)
- ongoing maintenance of sites and equipment (and capital refresh over time).

Some of this new investment to establish a dedicated PSMB network would represent ‘fixed costs’. That is, the investment will need to be incurred irrespective of the amount of traffic that is expected to be carried on the network — for example, the costs of establishing the initial coverage layer of the network. The same scale of investment would not be required under a commercial approach (or to a lesser extent a hybrid approach) because mobile carriers have already incurred these fixed costs (Optus, sub. 18).

A commercial operator could likely exploit greater operating efficiencies

There are significant costs associated with the ongoing operation of mobile networks, including the operation, maintenance and periodic upgrade of sites and site equipment, transmission networks, and core network systems. There are also significant organisational-level costs, including those associated with administration, service and labour force management, and accommodation (Optus, sub. 18; Telstra sub. 19; Victorian Government, sub. 28).

Many of the operating costs incurred by mobile carriers (both at the network and organisational-level) are likely to be largely invariant to PSA traffic (fixed costs) — for example, costs associated with maintaining site equipment, core network elements and billing platforms (Motorola, sub. 12). Accordingly, by exploiting economies of scale and scope, mobile carriers are expected to be able to minimise PSMB operating costs relative to a dedicated network operator (who would need to incur the aforementioned fixed costs).

That said, it may be feasible to achieve some scale efficiencies under a dedicated network approach by contracting out operation and maintenance activities to mobile carriers.

A dedicated approach could face more constraints on future spectrum inputs

Spectrum is a limited resource. Much spectrum in bands suitable for LTE has already been allocated or licenced, and a signification portion is held by mobile carriers. The large amount and mix of spectrum, cell types and technologies held by mobile carriers affords them considerable flexibility in terms of how they meet demand for network capacity.

There is no technical reason why an 'optimal' mix of infrastructure and spectrum could not be used to deliver PSMB services under a dedicated network approach. However, it could be more difficult to achieve an optimal mix under a dedicated approach if suitable spectrum is not readily available. Possible reasons for this include the appropriate band of spectrum not being available at the right time, or its potential acquisition not aligning with budget approval cycles and funding capabilities of governments. This, in turn, could mean that a dedicated network operator is not able to add capacity as cost effectively as a mobile carrier.

Irrespective of the delivery approach to PSMB, the valuable and scarce nature of spectrum resources heightens the need to use it as efficiently as possible, such as through flexible arrangements that allow it to be shared. Under any delivery approach for PSMB, efficient pricing and licensing frameworks can facilitate the sharing of spectrum resources with other potential users to reduce the risk of it sitting idle (chapter 7).

DRAFT FINDING 5.1

The costs of delivering PSMB under any option can be reduced by:

- maximising use of existing infrastructure
- sharing network capacity among PSAs in real time (that is, a non-partitioned network)
- allowing for flexible use of spectrum across users.

Extending mobile coverage will be costly under any approach

Some participants have suggested that a PSMB capability should extend to areas of Australia where there is currently no commercial mobile coverage, but there is LMR coverage (NSW Telco Authority, sub. 30; Victorian Government, sub. 28). There are several ways to deliver a PSMB capability to these areas.

- A dedicated approach would involve building a new LTE network for PSAs, with dedicated spectrum. Some use of existing infrastructure (such as LMR sites) may be possible.

- A commercial approach would involve paying a mobile carrier to extend its network in a way that meets PSA needs.
- A hybrid approach could take many forms — for example, a new network could be constructed and operated by a mobile carrier, but using government-owned assets.

However, providing a permanent PSMB capability in areas outside of the commercial mobile footprint would be extremely costly, irrespective of the delivery approach. It is highly unlikely that the benefits of a PSMB capability would justify these costs (although small-scale, targeted extensions may be warranted in particular circumstances). Indeed, BAI (sub. 1, p. 2) submitted that:

> In the less densely populated areas of Australia it is not, and never will be, viable to establish a high speed communications coverage network using PSMB, VHF, UHF or cellular terrestrial options.

This reflects the significant new infrastructure required, which would be costly. For example, according to some estimates, the costs of building a new base station site is in the order of 3 to 7 times more expensive than deploying new equipment to an existing base station. It would also involve the ongoing costs of operating and maintaining this infrastructure. Further, the cost of achieving a unit increase in population coverage (say from 99.5 per cent to 99.6 per cent) is expected to increase exponentially as a proportionally larger increase in geographic coverage is required) (figure 5.3).

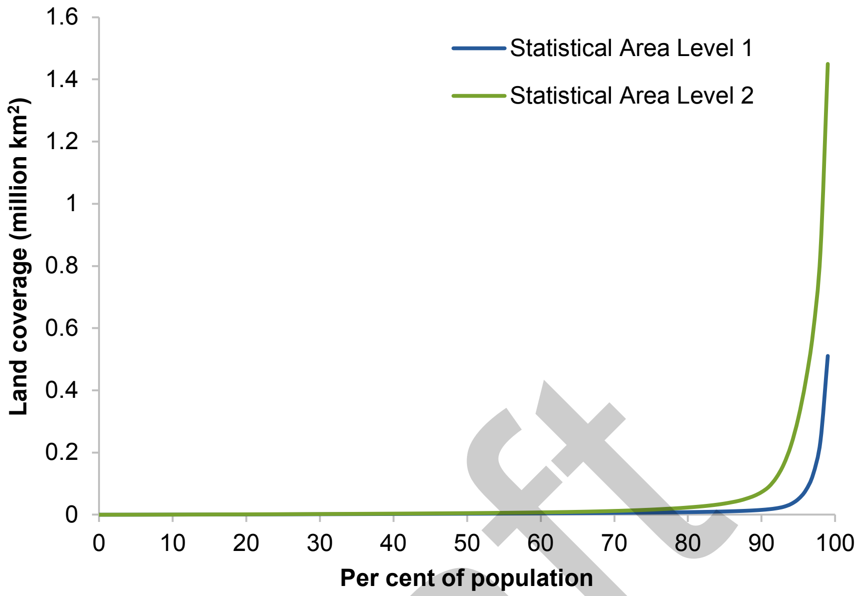
However, there are ways to deliver a level of broadband capability in areas outside the commercial coverage footprint (albeit not to a 'mission critical' standard) without extending LTE networks.

For example, transportable equipment — known as 'Cells on Wheels' (COWs) — provides temporary mobile broadband coverage in specific regions when it is needed. Commercial mobile carriers, and LMR network operators, already rely on transportables to extend the coverage and capacity of their networks on an as-needs basis. PSAs could use their own COWs and spectrum to provide temporary coverage, or they could engage this capability through mobile carriers.

Because of the inherent flexibility in when and where COWs are deployed, they provide a relatively low-cost way of providing network coverage and capacity in localised areas. They are particularly suitable for large planned events (such as music festivals), and may also be useful for dealing with medium to long-term emergency situations (such as a flood and recovery scenario). On the other hand, the fact that it takes time to deploy transportables to areas where coverage is required will limit their effectiveness in some emergency scenarios.

Figure 5.3 **Land coverage for percentage of population covered**[a]

Illustrative example



[a] Statistical Area Level 1 and Statistical Area Level 2 are spatial units in the Australian Statistical Geography Standard.

Data source: ABS (*Australian Statistical Geography Standard (ASGS): Volume 1 - Main Structure and Greater Capital City Statistical Areas*, July 2011, Cat. no. 1270.0.55.001; *Socio-economic Indexes for Areas (SEIFA), Data Cube only, 2011*, Cat. no. 2033.0.55.001).

Another alternative is satellite broadband. Satellite networks are used by mobile carriers to provide mobile voice and data services, and commercial investment in this platform is ongoing (Optus, sub. 18). Satellite technology has also been used by mobile carriers in emergency situations to provide voice and data services as a back-up while terrestrial services were being restored (Optus, sub. 18), and satellite voice services are already used by PSAs outside LMR coverage areas.

Relying on satellite broadband could be more economical than using transportable equipment. Moreover, satellite services can be accessed in any geographic area relatively quickly, where commercial arrangements are already in place. However, there are quality issues that need to be considered. For example, time-sensitive applications may not perform as well on satellite networks, and performance can be affected by weather conditions or the presence of smoke. That said, the next generation of satellites — such as those being deployed by NBN Co, the first of which is due to be deployed in 2015 — will provide greater capability than current generation satellites (Department of Communications 2015a; NBN Co 2015b).

New technologies also have the potential to change the economic case for extending permanently deployed mobile coverage into the future. For example, RF Technologies (sub. 3) indicated that a new technology it is developing would allow the delivery of PSMB using existing spectrum already used for narrowband (LMR) networks via incremental upgrades of the equipment in these networks. VHA (sub. 11) also indicated that the spectrum already owned by PSAs (in the 400 MHz band) could be used for LTE deployments, and that this is starting to occur in other countries.

DRAFT FINDING 5.2

Providing a permanent PSMB capability in areas not currently covered by commercial mobile networks would be very costly. There are lower-cost options that can be pursued to provide a level of mobile broadband coverage and capacity (such as transportable equipment or satellite broadband), albeit not to a 'public safety' standard.

5.4 Delivering a preferential service capability

Where PSMB is delivered using a commercial mobile network (under a commercial or hybrid approach), PSAs will need to be treated preferentially relative to other users on that network. Two issues are important:

- network accessibility — the ability for PSAs to gain initial access to the network in a timely (almost instantaneous) manner, even if the network is already congested
- priority services — the ability for PSAs to be prioritised over other traffic once they are on the network, such that they can utilise sufficient levels of network capacity.

Views differ as to whether network access can be 'guaranteed'

Some participants have questioned whether commercial network operators can provide 'guaranteed' network access to PSAs without dedicated spectrum (ACT Emergency Services Agency, sub. 25; MFB, sub. 6; NSW Telco Authority, sub. 30). For example, the MFB (sub. 6, p. 3) indicated that:

> MFB would support dedicated spectrum, rather than a hybrid model, because relying on private carriers to have available the required spectrum in wide-ranging emergency events would not be feasible. MFB is keen to avoid a scenario where, once the maximum dedicated spectrum is used, PSAs could not be given priority (on the mobile network, if you haven't connected, the system doesn't know you're trying to achieve access).

Specifically, concerns have been raised about the ability of LTE networks to:

- handle multiple simultaneous access requests during a major incident — if access requests exceed the amount that an LTE network can feasibly manage, a probabilistic process is used to determine accessibility, potentially meaning that only a small proportion of total access attempts are successful

- establish a call connection within a minimum acceptable timeframe (latency) (NSW Telco Authority, sub. 30).

Other participants and technical reports have indicated that it is possible to provide priority network access for specified users over LTE networks (Borkar, Robertson and Zdunek 2011; Ericsson, subs. 10 and 26). On this issue, Ericsson (sub. 26, p. 3) submitted:

> [T]hese technologies [for prioritising and pre-empting access to congested LTE networks] exist and Ericsson's Public Safety LTE offers Dynamic Prioritization and Pre-emption. Public Safety LTE systems immediately prioritize those users most critical to serving an incident, de-prioritize nonessential users and, when necessary, pre-empt. 3GPP support for this capability has been available for several years …

Several methods of controlling network access requests on an LTE network have been identified, including:

- restricting the frequency of access attempts made by commercial users through LTE's 'access control' function. In this case, access attempts from non-essential users or applications are restricted to reduce congestion to more manageable levels, making way for special classes of users (such as PSAs) to access the network (Ericsson, sub. 26; Motorola, sub. 31)
- forms of 'pre-emption', such as where a network refuses to permit new connections unless the access seeker is a member of a particular access class, or where commercial access classes are shut down based on pre-agreed triggers to make room for PSAs (Rivada Networks, sub. 9).

That said, it is not feasible to expect that any quality of service characteristic (including network access) can be delivered 100 per cent of the time, irrespective of the delivery approach. In practice, PSAs will need to consider what level of assurance they are seeking with regard to network accessibility, taking into account the relative benefits and costs.

Prioritisation is technically possible on commercial networks

The ability to categorise and prioritise users is inherent within existing LTE technology (Alcatel-Lucent, sub. 15; Ericsson, sub. 10; Motorola, sub. 12). LTE technology standards allow a particular user or application to be prioritised over others, and (in some circumstances) in real time (box 5.5).

No mobile carrier in Australia currently offers a priority data service for PSAs

Mobile carriers already prioritise some types of traffic and applications. For example, it has been standard practice (at least on 2G and 3G mobile networks) for voice traffic to take priority over data traffic, primarily because of the risks that latency presents to the quality of a voice call. For the PSA sector, this means that the National Emergency Call Service

(Triple Zero), and Wireless Priority System Service (WPSS) already receive priority over data services on mobile carrier networks (Telstra, sub. 19).

Box 5.5 **How does prioritisation work in LTE technology?**

All commercial users on an LTE network are categorised to a randomly allocated 'access class' (between one and ten) based on the SIM or USIM card in their device, with special access classes (between 11 and 15) for high-priority users (including one for emergency services) who can have a higher 'quality of service' (QoS) attached to their data traffic.

A 'bearer' is the term used to describe a 'virtual' channel established between the endpoints of an LTE network (from the end-user device to the core network). It is the means by which the network operator can differentiate one user's traffic from another (such as between a PSA and commercial user) and one application's traffic from another (such as a video stream compared to a web browsing session).

There are two types of bearer in LTE: default and dedicated. Every end user has at least one default bearer that is established when the end-user device first attaches to the network and remains available for the duration of the connection. An end-user device can have anywhere from zero to several dedicated bearers established at any given time and each is set up and taken down on an as-needed basis. Dedicated bearers are used when the QoS requirements for some traffic is different than the QoS provisions provided by the default bearer.

Each bearer (whether dedicated or default) is associated with two parameters: a Quality Class Identifier (QCI) and an Allocation and Retention Priority (ARP). The QCI parameter dictates the packet level preferential treatment a bearer receives, while the ARP parameter dictates the preferential treatment an individual bearer receives when they are being established. During periods of congestion, the network may need to make decisions regarding which bearer requests should be accepted and which should be rejected, and may also choose to drop bearers of low priority to free up required resources. The primary role of the ARP parameter is to facilitate this decision-making process — it ensures that the request of the bearer with the higher priority level is given preference over lower priority bearers.

Sources: Hallahan and Peha (2013); Borkar, Robertson and Zdunek (2011).

Some participants indicated that priority *data* services are already being provided to some business customers in Australia (Telstra, sub. 19). A priority data service for PSAs was trialled by Telstra at the G20 Leader's Summit in Brisbane in 2014. This capability (referred to as LANES — box 5.6) provided PSAs with a dedicated 'lane' of spectrum and the ability to overflow with priority onto Telstra's commercial network. However, the Commission is not aware of any examples of Australian mobile carriers providing priority for PSAs over LTE networks on a permanent basis (MFB, sub. 6; Victorian Government, sub. 28). Internationally, there is at least one example of priority services being delivered to PSAs — in Belgium, PSAs receive a limited priority data service on all three of the mobile carrier networks they rely on (appendix B).

While various commercial propositions for delivering prioritised PSMB over mobile carrier networks have been drawn to the Commission's attention, these are based on the presumption of some dedicated network (using dedicated spectrum) (box 5.6).

Box 5.6 **Commercial technology for delivering priority services to public safety agencies (PSAs)**

Telstra LANES technology

Telstra LANES is a unified national approach that involves integrating spectrum set aside for a PSMB capability into the architecture of the Telstra commercial carrier network so that it can form a seamless and reliable service for PSAs. This network could then be hardened through government investment to meet desired resilience requirements. Under the Telstra LANES model, spectrum set aside for PSMB is partitioned for PSA use only. PSA-only partitioned spectrum is then augmented with prioritised data on the carrier LTE spectrum in LTE coverage areas. Under a Memorandum of Understanding signed in 2014, Telstra's LANES capability will draw on technology developed by Motorola Solutions, which provides the capability for dynamic prioritisation.

Rivada Networks

Rivada Networks (sub. 9) has put forward a model for delivering a PSMB capability using dedicated spectrum (30 MHz of spectrum in the 700 MHz band). Priority would be managed using 'ultra-priority access' and 'ruthless pre-emption technology' designed by Rivada. This includes the use of Rivada's spectrum sharing technology, which would make bandwidth available instantly to PSAs when they need it. At other times, network capacity would be leased to other parties (on a wholesale basis) when not in use by PSAs, in order to facilitate competition and allow for more efficient use of spectrum.

Sources: Rivada Networks (sub. 9); Telstra (sub. 19; 2014a).

Levels of priority can be either statically or dynamically assigned

Some participants have indicated that providing a statically configured high priority channel for PSAs may not lead to the most efficient use of resources, as the priority a user needs will increase or decrease depending on their role or the incident they are attending (Ericsson 2014b; Motorola, sub. 12). Moreover, some participants have indicated that PSAs should be in the position to directly control which of their users and applications get priority, and be able to dynamically modify these arrangements during incidents (ATF, sub. 4; PFA, sub. 8, chapter 4). An alternative approach could involve PSAs establishing contractual arrangements with a mobile carrier which establish detailed set of protocols about how PSAs want priority arrangements to work in different situations. As part of this, it could then be open for PSAs to specify how they should be engaged throughout an incident to have control over critical aspects of communications.

The Commission understands that it would be technically feasible to prioritise individual PSAs users in a pre-defined static way or in a dynamic way based on individual users with LTE technology (Ericsson, sub. 26; Rivada Networks, sub. 27). However, it is less clear whether the current set of LTE standards support other aspects of dynamic priority, such as prioritisation on the basis of incident type, user role and location. Motorola has submitted that 3GPP support for these more sophisticated types of dynamic priority is currently limited, although solutions are in development (Motorola, sub. 31).

INFORMATION REQUEST

To what extent do current LTE standards support dynamic adjustment of the prioritisation of users or applications in real time? Can dynamic adjustment of prioritisation be on the basis of a user's role, agency or location? Using non-proprietary technology, is it possible for dynamic prioritisation to feature in commercial delivery approaches?

5.5 Network reliability

The ability for mobile networks to continue to operate in adverse conditions, to a high level of certainty, is considered a core element of delivering a PSMB capability (chapter 4). Reliability is largely a function of the resilience and robustness of the underlying infrastructure used to deliver mobile broadband services, how the network is managed and the effectiveness of fault restoration measures. The ability for PSA users to switch to alternative networks if the primary network fails can also be important.

Features of LMR networks which promote reliability

Network reliability is typically measured in terms of 'availability' (Ericsson, sub. 10; Motorola, sub. 12) — either in terms of individual network elements (such as individual sites) or end-to-end network availability (such as over a day, month or year).

LMR networks used by PSAs are designed to provide very high levels of availability (chapter 4). Participants have indicated that LMR networks have various features which make them inherently more reliable than commercial mobile networks.

- LMR sites are often targeted for hardening to make them less susceptible to damage during fires, floods and other natural disasters (NSW Telco Authority, sub. 30).
- LMR sites typically have back-up power supplies for 12-48 hours at each site, and up to 2-5 days for hard-to-access sites, compared to around 3-4 hours at a mobile carrier site (Alcatel-Lucent, sub. 15; Ericsson, sub. 10; Motorola, sub. 12; Victorian Government, sub. 28).
- LMR sites typically have multiple backhaul paths at each site (ATF, sub. 4; Motorola, sub. 15), which is not always the case for mobile carrier sites, particularly in low density areas (Alcatel-Lucent, sub. 15; Optus, sub. 18).
- LMR networks have highly proactive and reactive restoration measures in place, including undertaking repairs in a matter of hours, even in regional and remote areas (NSW Telco Authority, sub. 30).

Participants pointed to Australian and international examples where mission critical LMR networks continued to operate during emergency incidents where mobile carrier networks did not (ATF, sub. 4; NSW Telco Authority, sub. 30; PFA, sub. 8).

Mobile carrier networks can be modified to improve reliability

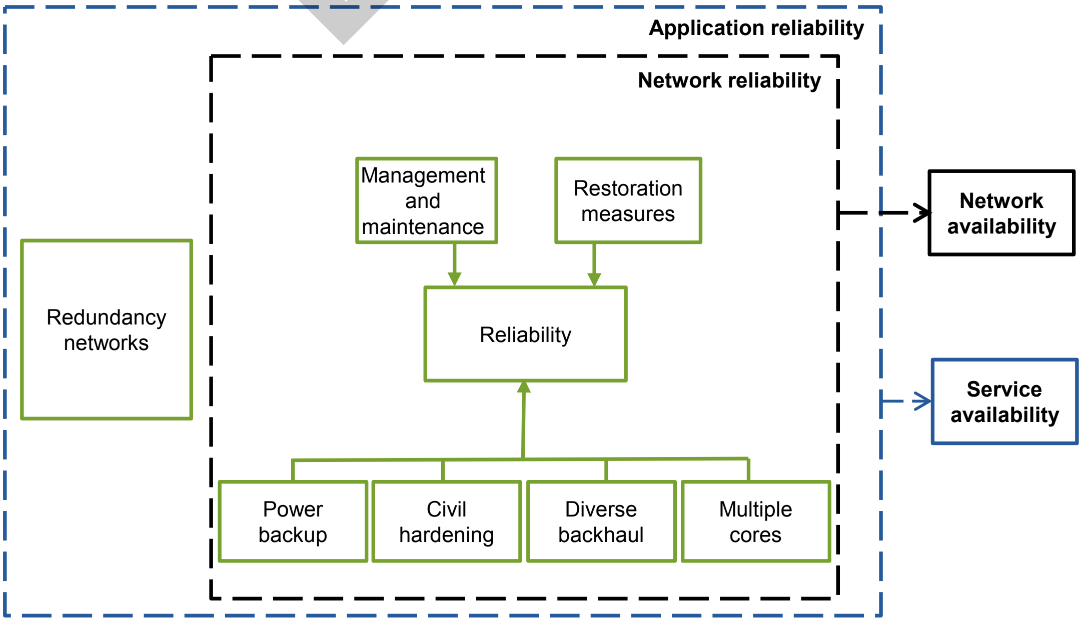
There was broad consensus among participants that mobile carrier networks would require a process of 'network hardening' to meet the requirements of a mission critical PSMB network. In practice, what this precisely entails, and how a particular set of hardening arrangements would translate to specific reliability measures, is a more complex matter.

There are various ways to harden mobile carrier networks

There are various inputs which contribute to the overall level of network reliability and which fall under the category of 'network hardening', including (figure 5.4):

- adding extra power backup, particularly to mobile carrier sites which are harder to access in the event of a natural disaster or incident
- civil upgrades to make key sites more resistant to floods, fires and sabotage, such as the possible raising of equipment to avoid flood damage
- adding alternative path (redundant) backhaul links to sites which do not already have geographically diverse backhaul
- ensuring that there is adequate redundancy built into the core network.

Figure 5.4 **Achieving reliable services for PSAs**



The Government Wireless Network in Queensland provides an example of a network approach designed to meet the specific needs of PSAs, including levels of resilience, while using existing mobile carrier infrastructure (box 5.7).

Box 5.7 The Queensland Government Wireless Network

The Government Wireless Network (GWN) is a mission critical P25 trunked digital radio network that provides secure radio communications for Police, Fire and Ambulance services in Brisbane and South-East Queensland. The network is provided under a managed service arrangement with Telstra, which is responsible for the design, build, operation and maintenance of the network over a 15 year period from 2014. Much of the infrastructure used in the GWN Radio Access Network is co-located on commercial cellular infrastructure.

Sources: Queensland Treasury (2015); Telstra (sub. 19).

Aside from individual network hardening, further redundancy can be offered by providing PSAs with access to alternative networks in the event of a network outage. For example, some participants noted an approach which draws on the infrastructure of multiple mobile carrier networks to minimise the risks of a single point of failure, and potentially reduces the extent of investment needed in other network hardening (Coutts Communications, sub. 20; CSIRO, sub. 16; Optus, sub. 18; VHA, sub. 11).

There is no technical limitation that prevents mobile carriers from hardening their networks to meet whatever service requirements are sought for PSMB (Ericsson, sub. 10). Telstra (sub. 19) argued that mobile carrier networks can be hardened to meet any resilience requirements, and far more readily than building a new dedicated network.

LTE networks offer greater reliability than earlier technologies

Several features of LTE networks mean they are likely to be inherently more reliable than previous mobile broadband technologies such as 2G and 3G networks for delivering PSMB (3GPP 2015b; 4G Americas 2013; Ericsson 2014b; SCF Associates 2014). In particular, LTE networks:

- typically use a large number of small cells in a dense configuration in highly populated areas, giving them a degree of site redundancy
- have the capability to operate as ‘self-organising networks’ that can self-configure (new base stations can be inserted into an LTE network and will work immediately), self-optimise (a site will operate to best meet the needs of the overall network) and self-heal (the network will automatically re-configure to cope with problems)
- have lower power demands than earlier technologies, meaning that backup power supplies last longer or that batteries can be deployed at cell sites rather than generators.

Future international technical standards for LTE are expected to further improve the reliability of LTE networks further (box 5.3).

The degree of network hardening could be influenced by the PSMB delivery approach

Any delivery approach for PSMB would be most efficiently delivered by leveraging existing infrastructure (including mobile carrier sites) to the maximum extent possible (section 5.1). However, hardening may not be a one size fits all approach, with different types of hardening needed in different areas (for example, a bushfire prone area compared to a cyclone prone area) (BAI, sub. 1), and for different types of sites (NSW Telco Authority, sub. 30). The type and extent of network hardening could also be influenced by the delivery approach to PSMB.

Telstra (sub. 19) argued that hardening an existing mobile carrier network would be less costly than building an equivalent level of redundancy into a new network. This could be, in part, because the dense cell configuration of mobile carrier networks (particularly in metropolitan areas) and mix of technologies used by mobile carriers may provide greater redundancy in the event of equipment and network failures.

On the other hand, the prospect of using a greater proportion of government-owned LMR sites in a dedicated approach, raises the potential for incremental hardening costs to be lower at these individual sites relative to mobile carrier sites (NSW Telco Authority, sub. 30). The degree to which a dedicated network approach could leverage existing LMR and other government-owned sites would likely differ across jurisdictions (section 5.3).

Due to a lack of detailed information on the reliability of existing commercial and government-owned networks, and the mix of sites that would be used within any given jurisdiction, it has not been possible to identify incremental hardening requirements, and the extent to which they would differ across delivery approaches.

Roaming across multiple networks to promote greater redundancy raises potential benefits and challenges

Roaming technology allows customers of one mobile carrier to use the network of another, with systems keeping track of data usage and billing (Alcatel-Lucent, sub. 15; Ericsson, sub. 10; Rivada Networks, sub. 9). For example, in Australia, VHA has entered into arrangements with Optus for its customers to roam on to the Optus network in some regional areas.

Roaming across networks offers several potential benefits for delivering a PSMB capability compared to an approach which relies only on a single network. The potential benefits include PSAs being able to access additional coverage or capacity (section 5.3), and the overall network solution offering PSAs greater reliability because there are multiple networks in place if one is unavailable (CSIRO, sub. 16; Optus, sub. 18; VHA, sub. 11). By extension, the degree of network hardening required in a multiple carrier approach could be lower (Optus, sub. 18; VHA, sub. 11).

Potential challenges with a multiple network approach also need to be considered. It would require the establishment of roaming arrangements between networks, such as between mobile carriers. Some participants have indicated that an approach which involves roaming between multiple networks introduces the risk that the PSMB capability provided to PSAs will not be 'seamless' where a call (or data session) has to be disconnected and re-authenticated as network boundaries are crossed (NSW Telco Authority, sub. 30; Telstra, sub. 19). Some of these challenges are evident in arrangements for roaming between LMR and LTE networks today (box 5.8).

Box 5.8 **Roaming between LMR and LTE networks**

There are examples of roaming arrangements established between LMR and mobile carrier networks. For example, devices connected to the Metropolitan Data Network (MDN) in Melbourne will automatically switch to the Optus network (where available) when the connection with the MDN is lost. However, the application session will be interrupted as the new connection is established and authenticated, resulting in a break in data transmission. This is likely to be an issue for real-time applications, such as live video or voice communications, as the user experience might not be up to the standards that PSAs require.

Source: VDTF (2015b).

There are different types of roaming arrangements, with different quality standards attached (box 5.9). The Commission understands that establishing roaming arrangements between multiple networks is technically feasible, as is the implementation of measures to ensure that there is continuity of services in delivering a PSMB capability (Alcatel-Lucent, sub. 15; Ericsson, sub. 26).

However, there would also be costs. First, each participating mobile carrier would need to ensure that their network has the capability to recognise PSA traffic and, where relevant, the ability to provide them with preferential services. This could be a more complicated task than when using a single carrier, and could require some mobile carriers to upgrade their existing core networks and systems. Second, roaming agreements will need to be established between mobile carriers, with the necessary technical upgrades to support roaming put in place. The higher the standard of roaming capability sought, the larger the costs and complexity which are likely to be involved (Telstra, sub. 19).

Ultimately, the desirability of a multiple carrier approach will also depend on the type of arrangements that are being sought. If the desired approach is for PSAs to have access to multiple networks with the same quality of service standards across each network, there may be greater technical considerations and costs involved. On the other hand, if the desired approach is to rely largely on a primary network for delivering the main PSMB capability, with the ability to use other mobile carrier networks in the event the primary network is unavailable, PSAs may be more comfortable with trading off some level of service quality.

Box 5.9 There are multiple ways to implement roaming

LTE standards allow for two types of roaming.

- International roaming — where users 'visit' a mobile carrier's network when abroad, receiving similar levels of coverage and service as the network's domestic users.
- National roaming — where users on one mobile carrier's network can undergo 'handover' to another mobile carrier's network.

Each of these roaming arrangements could be used to deliver a PSMB capability, but with differing service levels.

International roaming allows users to connect to another network and receive an experience that is similar to that of the network's 'home' customers. Despite the name, a multiple carrier PSMB network could use international roaming by providing PSAs with SIM cards that 'trick' the network into thinking they are international users (an approach used in Belgium's Blue Light Mobile network). However, switching between networks under international roaming is not seamless, requiring termination of the old network connection before searching, accessing, and re-authenticating on another network — a process that can take minutes.

National roaming offers scope for a more seamless handover of users between LTE networks, although precisely how seamless will depend on the level of integration between the two networks, and the type of applications to be supported. For basic applications (such as internet access), one possible method is to define the neighbouring cells of both networks in each mobile base station (eNodeB). In simple terms, this makes the base station aware of all the surrounding cells (of both networks) to which a handover can made. Another is to enable IP-connectivity between the two networks, which allows for the Automatic Neighbour Relations feature of LTE to automatically find (and handover to) other cells in real-time. More complex applications such as voice over LTE may also require support from the end-user device, chipset or the application vendor to fully implement roaming arrangements between multiple mobile networks.

Any roaming solution requires co-ordination and integration between mobile carriers, which could be costly (although dependent on the applications to be supported), limit the carrier's ability to independently configure their networks in the future without consideration of the supported interconnection, and may impact on existing commercial users.

Sources: Alcatel-Lucent (2010); Gras (2015); FCC (2010b); NMC Consulting (2013); NSW Telco Authority (sub. 30).

5.6 Interoperability and security

Sharing the right information with the right people is central to how PSAs operate. Communications technologies need to be interoperable to enable information sharing, whether across PSAs within a jurisdiction or between PSAs in different jurisdictions. Communications also need to be secure from interception or disruption.

Broadband technologies can support interoperability

Historically, the use of incompatible (and often proprietary) technologies for LMR networks has limited interoperability across agencies and jurisdictions (chapter 2). The spectrum bands, software or end-user devices used on one network have not always been compatible with those used on another, even where both networks have been built under the same technology standard (such as Project 25 standards).

To address these legacy problems, jurisdictions agreed to a timetable for transitioning towards interoperable technology over the period 2010–2020 (under the *National Framework to Improve Government Radiocommunications Interoperability*). These efforts are being supported by ACMA's consolidation of public safety radio communications into part of the 400 MHz spectral band (ACMA, sub. 14). Some jurisdictions have also moved towards managing emergency services from a whole-of-government perspective, including to improve interoperability between agencies (NSW Telco Authority, sub. 30; Victorian Government, sub. 28).

The advent of PSMB offers a significant opportunity to avoid interoperability problems in the future. This is because mobile broadband technology is largely standardised at the international level, which can facilitate interoperability across a large number of users and systems — regardless of the specific delivery approach chosen. Separate to this, there is also scope for PSAs and jurisdictions to collaborate with one another to facilitate interoperability prior to the implementation of a PSMB capability (chapter 7).

International standards facilitate interoperability

Mobile broadband technologies have several features that allow for interoperability between applications, devices and networks, regardless of the specific network design and/or equipment manufacturer. Both LTE and 3G technologies are backed by open-source international standards that are widely supported by the majority of manufacturers of network equipment and end-user devices. In addition, LTE is based on internet protocol, the method of encoding and transferring data in 'packets' that underlies all internet-connected devices and networks. Participants pointed to the potential for LTE technology to support a high degree of interoperability across PSAs and jurisdictions (for example, Rivada Networks, sub. 9).

It would be possible to achieve a high degree of technical interoperability between networks under any PSMB delivery approach — provided that common standards are adhered to across PSAs and jurisdictions. This will be important as the future introduction of proprietary features or technologies could compromise interoperability (Alcatel-Lucent, sub. 15). However, there may be some technical differences across delivery approaches in how interoperability is achieved, including whether PSA users can switch seamlessly between different networks, and how their communications would be prioritised on another network (section 5.4).

The choice of end-user devices (such as handsets and in-vehicle terminals) will also matter for interoperability in each delivery approach. In a dedicated approach, end-user devices would need to operate on the spectrum used on the network (section 5.2). The devices used by one PSA or jurisdiction would also need to be compatible with the spectrum bands used by other PSAs or jurisdictions (where there is a need to interoperate).

These considerations also influence the cost of procuring end-user devices. There is already a large global market for devices, with manufacturers able to spread their development costs over a global customer base (economies of scale) and facing commercial pressures to innovate and adopt new features. Drawing on this market to supply PSAs is likely to result in lower overall costs compared to the procurement of customised devices (Telstra, sub. 19). This could involve 'ruggedising' retail devices to meet PSA needs (by making devices resistant to heat, pressure or water) or procuring devices that have been developed to meet PSA needs internationally (although the ability to do this would depend on the costs of adapting these devices to support the spectrum bands used).

Moreover, the wide range of LTE-suitable spectrum bands supported by many retail devices offers a further opportunity to facilitate roaming across networks, and hence interoperability. In a commercial approach (or a dedicated or hybrid approach with spectrum in a suitable band), this could also give PSAs the ability to adopt a 'bring your own device' policy and reduce the number of end-user devices they need to purchase — for example, where SES or rural fire agencies allow their volunteers to use their own mobile phones on the PSMB network (CDMPS et al., sub. 7). Further, by using the same technical standards as many consumer devices and applications, PSAs may be better placed to engage in intelligence gathering and mass communication with the wider public (Telstra, sub. 19).

However, there are risks to technical interoperability under any PSMB delivery approach. Delays in the finalisation of international standards for some LTE features — such as mission critical voice — could increase the risk of proprietary solutions being 'locked in' that compromise future interoperability. Different deployment timelines across jurisdictions could mean that new standardised features are adopted sooner in some places than in others, potentially hindering the ability for PSAs to roam onto the networks used by other agencies or jurisdictions (Telstra, sub. 19). This could also be a risk in any approach that involves multiple mobile networks, which would inevitably present co-ordination challenges when new standards become available.

These risks will need to be managed carefully. There may be a need to coordinate technology upgrades or end-user device choices across networks or jurisdictions. Alternatively, technology upgrades could be implemented in a way that allows for 'backwards compatibility' with earlier standards or technologies (a feature of many 3GPP standards). Individual agencies and jurisdictions will also need to consider the extent to which their software systems (such as applications or encryption technologies) can or should be compatible with those used by others.

In the Commission's view, common technical standards are a necessary but insufficient condition for facilitating interoperability of a PSMB capability within and across jurisdictions. A range of other matters will need to be addressed at the institutional level, including arrangements for sharing information among agencies (chapter 7).

DRAFT FINDING 5.3

There are technical and institutional barriers to interoperability that will need to be overcome.

- Technical interoperability across mobile broadband networks requires compatibility of network equipment, end-user devices and software. A common and agreed set of technical standards can facilitate this.
- Agencies will need to develop protocols and procedures for storing and sharing information, both with other agencies in the same jurisdiction and with interstate counterparts.

Opportunities to integrate voice and data

Existing LMR networks for PSAs will likely remain in place for some years to come (section 5.7). However, as agencies make greater use of mobile broadband and new equipment is developed that incorporates mission critical voice functions (in line with international standards), an important question is whether it is possible for users to interoperate across both types of network — either on an ongoing basis, or as part of a transition to full reliance on PSMB for voice communications.

Coexistence between narrowband and broadband networks could be achieved through maintaining separate equipment (such as handsets and vehicle radios) that users would need to switch between, and by using 'dual-mode' equipment that can operate across both networks. The best approach may vary across PSAs or jurisdictions. While the precise technical considerations might vary across PSMB delivery approaches, the broad considerations are likely to be similar.

One consideration is cost. In principle, dual-mode equipment could be less costly in the long term if it means that the total number of end-user devices can be reduced. This could also have indirect impacts, such as reducing the risk of user error in mission critical situations, since personnel would not need to operate two different sets of equipment. However, each individual end-user device may be more expensive, especially if it needs to be customised to a specific type of existing narrowband network (or to multiple narrowband networks to facilitate interoperability across jurisdictions). The smaller global market for such equipment may also increase costs.

However, the ultimate arbiter will be what is technologically possible. Participants noted that end-user devices and network equipment (such as gateway and interface devices) that allow for interoperability across LTE and narrowband networks are already being manufactured (Ericsson, sub. 10; Motorola, sub. 12; NEC, sub. 5). These include systems that provide push-to-talk functions and those that give voice communications priority over other forms of data (such as the Group Radio Solution that enables interoperability between narrowband and 3G networks trialled by Telstra (2011a)).

There are technical challenges to the development of dual-mode equipment, and it may not be possible to link every type of LMR network with an LTE network. One challenge involves manufacturing devices that can operate across all the relevant frequency bands. A related consideration is the band(s) of spectrum used in a dedicated or hybrid PSMB approach, and whether it allows existing equipment to be used or whether it would require new equipment to be manufactured (with a consequent bearing on costs).

Moreover, the dual-mode handsets thus far developed are based on proprietary technologies that are not currently reflected in international standards for LTE — and many are not compatible with one another — although future standards releases may be able to accommodate some of these features (Ericsson, sub. 10; Motorola, sub. 12, 31). International standards and technology development will also play a key role in the timing of any transition of mission critical voice applications onto broadband networks.

Communications can be secured in a range of ways

Establishing and maintaining the integrity and security of communications is challenging over any network with multiple users and devices. This is especially the case for mobile broadband networks that involve a range of dispersed network infrastructure and end-user devices.

In essence, security refers to the prevention (and rectification) of two types of threat.

- Disruption — the risk that network functions or services are not available when they are needed, due to wilful or accidental causes (such as power outages, physical damage, equipment failure, network congestion, radiofrequency 'jamming' or cyber-attack).
- Interception — the risk of unauthorised personnel eavesdropping on sensitive communications, accessing databases (such as crime databases) or identifying the location of devices or network users.

Physical infrastructure is central to reducing the risks of disruption. This can involve, for example, restricting access to sites and other infrastructure to reduce the possibility for unlawful tampering. It could also involve installing equipment that can detect and compensate for radiofrequency jamming (Motorola, sub. 12), or actively monitoring for cyber-threats. Disruption can also be minimised by improving the reliability of networks (section 5.5) and through technologies that enhance the accessibility and priority of PSA communications (section 5.4).

Protecting communications from interception or the unauthorised retrieval of data generally involves a different set of measures. For example, while physical infrastructure can restrict physical access to network equipment, it is less useful in preventing unauthorised persons from intercepting communications sent over the radio 'air interface' or from remotely gaining access to network control systems or end-user devices.

At a minimum, protecting against interception and 'hacking' requires data to be encrypted. The most comprehensive method is 'end-to-end' encryption, which involves encrypting data travelling over the air interface and between different network components (such as backhaul and network cores) such that it can only be decrypted by the intended recipient. Participants emphasised the necessity of end-to-end encryption in a PSMB capability (for example, Motorola, sub. 12; Victoria Police, sub. 17), including over interoperable LMR networks (Motorola, sub. 31). In particular, Victoria Police (sub. 17) noted that a high level of security would be needed where commercial end-user devices are capable of operating in the same spectral band as a PSMB network.

Encryption technologies are already used across many IP-based networks — of which LTE is one example — and are continually being improved. For example, many mobile carriers offer Virtual Private Network solutions to their corporate customers to provide a secure connection between mobile end users and a company's secure internal networks (for example, Telstra 2015c). Some participants noted that existing technologies are likely to be sufficient for encrypting PSAs' communications (Ericsson, sub. 10), and that these are consistent with LTE standards (Rivada Networks, sub. 9).

Other techniques available to maintain the integrity and security of communications include:

- the use of authentication techniques to confirm the identity of devices (or their users), such that only authorised personnel can access public safety networks (MFB, sub. 6; Motorola, sub. 12)
- measures to secure data stored in the network core (including 'configuration' data relating to users' access and priority over the network) or in databases (whether in secure data centres or in 'the cloud'), such as isolating PSA data (Motorola, sub. 12, 31)
- limits on the linking of databases or networks, such as restricting access to secure internal networks and databases (thereby limiting scope for 'hacking').

Technologies to do these things are already widely available and have been deployed on commercial mobile broadband networks.

From a technological perspective, the security of communications is largely a matter of incorporating encryption technologies into end-user devices and some network core equipment. As a consequence, security is unlikely to have a significant bearing on costs across different PSMB delivery approaches (Ericsson, sub. 10).

PSAs would likely have a higher degree of direct control over network functions and security systems under a dedicated approach than under a commercial arrangement (section 5.3). However, even under a commercial approach, PSAs can retain control of how their communications are encrypted — PSA traffic may travel over commercial infrastructure, but commercial operators would not necessarily be able to decode or understand that traffic. Indeed, commercially built or operated networks are already used to carry sensitive traffic for defence, police and others (Telstra, sub. 19).

5.7 Timing and sustainability

Some aspects of a PSMB capability remain uncertain making it challenging to design and implement a PSMB capability by or before 2020 (a consideration set out in the study's terms of reference). Mobile communications technologies are evolving rapidly. Some capabilities are still being developed and are not yet widely available (such as mission critical voice communications over LTE). Others not yet thought of could become commonplace in the future. The cost of some equipment, and of delivering a particular capability, can rise or fall significantly over time. Added to this is considerable uncertainty about what applications PSAs will be using in the future, when they will adopt new applications, and what their data needs will be (chapter 4).

Several challenges would be involved in implementing a PSMB capability by or before 2020, some of which might vary depending on the delivery approach.

A dedicated network build would take time

On the infrastructure side, deploying new infrastructure and equipment takes time. A dedicated PSMB capability would involve installing new radio access network equipment and core network equipment — which would require significant work (proportional to the size of the network) and the availability of a skilled workforce.

Participants have indicated that a dedicated network will, by its nature, take the longest to implement (Motorola, sub. 12; Telstra, sub. 19). For example, Telstra (sub. 19) indicated that it takes around 1–2 years for mobile carriers to build initial network coverage and then a further year to extend it to a high proportion of the population, and that it is not unreasonable to expect a dedicated network to take significantly longer. Deployments of new mobile network technologies in Australia also provide some guide on the timing of a dedicated network rollout. For example, it took Telstra 3 years to build its LTE network to cover 87 per cent of the population, and another year to extend this to 94 per cent of the population (Telstra 2011b, 2014b, 2015a).

Another consideration is that spectrum cannot be obtained instantly. The implementation of a dedicated PSMB approach may need to be delayed until a formal spectrum allocation decision has been made by ACMA (and any such spectrum has been cleared of existing uses). This process could also depend on ongoing international processes to agree on harmonised spectrum for public safety (Telstra, sub. 19).

Some factors present challenges under all approaches

Other factors could influence the timing of deployment, and will apply to all PSMB delivery approaches.

- Some international standards are not yet in place. In particular, standards for delivering mission critical voice over LTE networks are still being developed (next section).
- All approaches will involve some level of commercial involvement, and designing and running tender processes and negotiating contracts will take time (at least 12 months).
- Governance arrangements will need to be established. This includes assigning responsibilities (or creating institutions) as to who funds the initial delivery of a PSMB capability and coordinates and takes decisions about future investments in additional capacity or coverage (chapter 7).

Voice and data services for PSMB are unlikely to converge on an LTE network before 2020

The convergence of mission critical voice and data communications onto a single PSMB capability using LTE technology before 2020 would be high risk under any delivery approach. In large part this is because the relevant international standards for mission critical voice on LTE are still being developed (box 5.4). Delays can also occur in the commercial development of equipment that reflects updated standards, due to the need to thoroughly test equipment and functions before deployment (Motorola, sub. 12). Key stakeholders do not expect any final standards to be reflected in manufactured equipment for at least another five years, and possibly longer (section 5.2). Implementation timetables vary across countries, but only the United Kingdom is anticipating full reliance on PSMB for voice communications before 2020 (appendix B).

A further challenge could arise from the willingness of PSAs to transition voice communications to mobile broadband given the risks and uncertainties involved, although this willingness could change over time as they gain more experience with using a PSMB capability and the relevant technologies mature.

Victoria Police (sub. 17) submitted that full convergence to a single PSMB platform would likely take a decade to implement, given that it is not yet clear whether such converged services would meet operational requirements. The Victorian Government’s Emergency Communications Plan envisages a transition away from LMR networks in the medium to long term, assuming that a PSMB capability can meet the necessary service standards (EMV 2014).

Participants also noted that existing delivery contracts for narrowband network infrastructure would be a major impediment to meeting a 2020 target for the delivery of PSMB for data *and* voice (Telstra, sub. 19; Victoria Police, sub. 17) — an economic rather than technical constraint. Participants have indicated that LMR networks will continue to be used (and upgraded as necessary) in the foreseeable future, particularly for mission critical voice capability — and even once technical standards are in place there is likely to be an incremental transition to LTE for mission critical voice.

This will reduce some of the risks associated with implementing a PSMB capability before 2020 as there is greater scope for newer voice-over-LTE technologies to be trialled and refined. For example, the NSW Telco Authority (sub. 30, p. 33) anticipates the commencement of PSMB voice capability from 2019, but:

> … with less critical voice services migrating first until confidence in the ability to provide mission critical voice services over LTE is established. Given these timeframes, it is expected that as part of the overall effort to rationalise assets and infrastructure, a partial refresh of existing networks and assets will be carried out in order to ensure that integration is successful.

Ultimately, the decision to integrate voice will depend on the individual circumstances in each jurisdiction. Some jurisdictions may eventually choose to decommission their narrowband networks in some areas as these networks reach the end of their economic life, and as voice-over-LTE technologies become available at a sufficient standard (Victorian Government, sub. 28). This could generate savings by avoiding maintenance and upgrade expenditures or allowing governments to sell (or lease) existing tower infrastructure or real estate, and avoid the risk that existing LMR networks are not supported by suppliers and industry over the longer term (NSW Telco Authority, sub. 30). It may also enable ACMA to consider the most valuable use of the relevant spectrum — for example, spectrum in the 400 MHz band (currently used for public safety narrowband networks) could be used to deliver LTE mobile services, either for commercial markets or PSAs (VHA, sub. 11).

However, jurisdictions may also opt to retain narrowband networks over a longer timeframe. This could be to provide a 'backup' communications capability for times when PSMB is not available (section 5.5), or in geographic areas that are outside the coverage footprint of a PSMB capability (section 5.4).

A flexible approach is more sustainable

Ultimately, the sustainability of a PSMB capability will depend on whether it can meet the needs of PSAs over a long period of time and whether it can do so at an acceptable economic cost. Making this happen poses considerable challenges given the high levels of uncertainty involved.

Policymakers will need to be flexible. In other areas of infrastructure and policy, a flexible approach that allows changes to be made quickly when new information becomes available, or for investment to be delayed, can help to minimise costs over the long term (PC 2011, 2012). It can also lead to more sustainable solutions that provide services to the community in the face of unexpected events. This is often referred to as the 'real options' approach to investment (chapter 7).

There are several ways to incorporate flexibility into the delivery of a PSMB capability. Maintaining consistency with international standards is one important way. This can keep costs down, facilitate interoperability and allow governments to switch suppliers over time as technologies or market conditions change (chapter 7). Past experiences with government-owned radio networks have shown that use of non-standardised (proprietary) technology and equipment can lock PSAs out of using new technologies that may be better or cheaper (chapter 2).

In addition, working with the private sector can help governments to quickly respond to, and make best use of, technological developments. Commercial networks have very large customer bases (relative to the number of public safety officers) and face commercial pressures to adapt to their customers' preferences and reduce costs, including by bringing new features to market as technology evolves (Telstra, sub. 19). PSAs can benefit from commercial network operator decisions to deploy new technologies or expand their capacity or coverage.

These dynamics present different risks and opportunities across PSMB delivery approaches. Maintaining adherence to international standards will be a challenge under all approaches but, as noted in section 5.5, any approach involving multiple networks may require some coordination of technology upgrades across networks. A dedicated approach would not necessarily face these risks, though it would not benefit from the pressures on commercial mobile carriers to upgrade their own networks, and hence there are greater risks that the technology used could become obsolete over time. For example, Telstra (sub. 19, p. 6) submitted that a dedicated approach ' … is more likely to involve a single vendor and proprietary solution which will limit choice and development options in the future'.

5.8 Summing up

The Commission's analysis finds that it is technically feasible to deliver a PSMB capability under a dedicated, hybrid or commercial approach.

Some technical challenges are common to all approaches, such as the need for network hardening to meet a given reliability standard, ensuring appropriate security arrangements are in place and ensuring that the technical basis exists to promote interoperability within and across PSAs. Other technical challenges could be exacerbated under some delivery approaches, such as the additional complexity that could arise from utilising multiple mobile carrier networks.

The following chapter evaluates the costs, risks and benefits of PSMB delivery approaches through a specific set of delivery options (chapter 6).

DRAFT FINDING 5.4

It is technically feasible to deliver a PSMB capability under a dedicated, commercial or hybrid approach. However, the ability of commercial mobile carriers to provide PSAs with 'guaranteed' network access and priority over other traffic without dedicated spectrum is yet to be demonstrated.

6 Evaluating PSMB options

Key points

- The Commission has evaluated the costs, benefits and risks of a specific set of delivery options for public safety mobile broadband (PSMB) to assess whether, how and why these might vary across options. Key cost differences have been evaluated quantitatively, whereas benefits and risks have been considered in a qualitative way due to a lack of robust data.
- Four options have been evaluated for areas of Australia with commercial mobile coverage: a dedicated network, two hybrid options (with varying levels of reliance on commercial networks), and a commercial option.
- A bottom-up approach has been developed to evaluate the network-related costs of each delivery option over a 20-year period from 2018. Key insights from the analysis include:
  - a commercial option is the most cost-effective way of delivering a PSMB capability to public safety agencies. Preliminary results indicate that a dedicated network is about 2½ to 3½ times more costly than a commercial option depending on the assumptions applied
  - a hybrid option is also more costly than a commercial option, though the cost difference narrows as the size of the dedicated network component decreases. However, even the lowest-cost hybrid option considered (with a dedicated network element in metropolitan areas only) is estimated to be about twice as costly as a commercial option.
- The relative cost differences between options are predominantly driven by more efficient use of existing infrastructure, including radio access network sites and backhaul transmission.
- The quantitative network cost results are sensitive to the design of the specific options and a number of the parameters and assumptions. However, the cost ranking of options is robust to the use of alternative inputs and assumptions.
- Nevertheless, costs are not the whole story. The nature and magnitude of risk varies across PSMB delivery options. For example, the risk of governments becoming ‘locked in’ to using a single supplier is most pronounced under a commercial option, while a dedicated approach is most susceptible to delays and technological obsolescence.
- While benefits have not been quantified in this study, the options under evaluation have been designed to deliver a similar level of PSMB capability. As such, the impact of each option on public safety outcomes (and thus its benefits) is not expected to vary markedly.
- The results of this analysis — in particular the quantitative component — are preliminary. The Commission is seeking detailed feedback on the methodology, assumptions and inputs used to refine this analysis further for the final report.

This chapter evaluates the costs, benefits and risks of alternative ways of delivering a public safety mobile broadband (PSMB) capability — including quantitative evaluation of the costs of different options. The aim is to identify and understand key cost drivers, risks and tradeoffs between options.

Section 6.1 describes the options that have been evaluated. Section 6.2 summarises the approach to estimating the costs of these options and the results (with further detail provided in appendix C). Section 6.3 evaluates the risks and section 6.4 the benefits of the options.

6.1 Options for evaluation

The terms of reference ask the Commission to consider three high-level approaches — a dedicated PSMB network, a commercial approach and a combination of both. In practice, these three broad *deployment approaches* could be defined in myriad ways, giving rise to a large number of feasible PSMB *delivery options*. The diverse models adopted internationally attest to this (appendix B).

It is not practical to evaluate all feasible PSMB delivery options in detail. Instead, a subset has been selected based on considerations that the options:

- are capable, as far as possible, of providing a 'public safety grade' mobile broadband capability — that is, a level of network capacity that can be scaled up as required, and a level of service quality that allows public safety agencies (PSAs) to use mobile applications in 'mission critical' situations (chapter 4)
- have regard to approaches being adopted in other countries
- have regard to approaches discussed in previous studies
- are able to be evaluated using publicly available information
- are technically feasible.

As noted in chapter 5, due to data limitations, the Commission's quantitative analysis of the costs of delivering a PSMB capability is focused on areas within the commercial mobile coverage footprint (for 3G mobile networks), or a target of approximately 99 per cent of the population. The Commission will consider extending its quantitative analysis for the final report if relevant information is forthcoming.

Some factors are common to all options

Based on the discussion in chapter 5 and consideration of study participants' views (hereon 'participants'), a number of factors are taken as common across all delivery options.

LTE technology is used

There is widespread agreement among participants that a PSMB capability should be delivered using Long Term Evolution (LTE) technology, regardless of the delivery option chosen (chapter 5). Accordingly, LTE is a common feature of each option considered. The assumption made in this study is that LTE coverage will reach at least an equivalent level of 3G coverage in the future and that 4G networks will eventually be used to deliver mobile voice services (Penn 2015).

That said, mobile networks are typically a collection of multiple technologies, and this mix changes over time. For example, commercial mobile carriers (hereon 'mobile carriers') currently operate 2G, 3G and 4G networks, use different types of cells in specific areas (macro, femto or pico cells) and at times use transportable cells (for example, during large planned events). This suggests that various technologies and platforms could be used to complement the delivery of PSMB, and the costs involved in doing so may differ across options.

Some existing network infrastructure is shared

Sharing existing infrastructure to the fullest extent possible avoids unnecessary duplication and reduces PSMB deployment costs, all else equal (chapter 5). In seeking to deliver a PSMB capability there are two key areas where 'network sharing' could lower the capital costs and ongoing operational costs of deployment:

- sharing radio access network infrastructure — this could include sharing 'passive' infrastructure at a site (such as space to put equipment, antennas/masts, power supplies and transmission capacity) or sharing 'active' equipment (such as spectrum, mobile base station equipment and existing backhaul capacity) (GSMA 2012; NEC 2013)
- sharing core network infrastructure — this could involve, for example, a 'Gateway Core Network' approach where the Mobility Management Entity element is shared between different mobile carriers, or more extensive forms of sharing which involve spectrum for a PSMB capability being fully integrated into a carrier's core network (Alcatel-Lucent 2009; GSMA 2012; Telstra, sub. 19).

The sharing of radio access network passive infrastructure is relatively common in parts of the mobile sector in Australia and in other countries, and there are significant opportunities for this given that there are over 15 000 mobile sites across Australia. Accordingly, all options are based on a high degree of sharing of existing physical sites and the purchase of transmission backhaul capacity from the existing commercial market.

Commercial networks are hardened

Participants have indicated that mobile carrier networks, as they are currently designed, do not meet the reliability requirements of PSAs (chapter 3). Accordingly, the need to 'harden' these networks to meet a higher level of reliability — through civil site upgrades, improved battery back-up and multiple transmission paths to each site — is a common feature of all options. This is because all options involve using or sharing commercial network infrastructure (such as mobile base station sites) to deliver PSMB.

The same standards of coverage apply

Any measure of coverage explicitly or implicitly attaches a standard of 'quality' to that coverage. For example, coverage measures can be based on the ability to receive an indoor signal (in-building coverage), an outdoor signal to a handset (handheld coverage), or outdoor coverage to a specially constructed vehicle antenna (vehicle coverage). Different standards of coverage may be required in different areas, for example, in-building coverage is likely to be critical in central metropolitan areas, while outdoor coverage may be sufficient in rural areas (chapter 5).

To compare options on an even keel, it is assumed that each option achieves the same standard of coverage in each geographic region. That is, indoor handheld coverage is assumed in dense urban, urban and suburban areas, and outdoor vehicle coverage is assumed in rural and remote areas.

Handset costs are assumed to be the same

The spectrum band used in delivering services to PSAs could be an important determinant of handset costs (chapter 5). Other things being equal, a spectrum band consistent with that used to provide commercial services would be expected to result in lower handset costs as PSAs could leverage off very large commercial markets for handsets. Where custom made PSMB handsets and devices are sought, there may be advantages in aligning the spectrum band used with that used in other international jurisdictions for PSMB.

For the purpose of the quantitative analysis a simplifying assumption has been made that handset costs will be the same across options, and that PSAs use a mixture of commercial devices, ruggedised handsets and in-vehicle terminals. However, some delivery options carry a higher risk that widely available (and cheaper) end-user devices are not able to be used (section 6.3).

PSMB capacity is used efficiently

Giving each PSA a fixed amount of network capacity over a PSMB capability (sometimes called a 'partitioned network') would likely mean that some capacity goes underutilised even where it may be of value to another agency. Sharing the available capacity among agencies in real time would be more flexible and reduce the total network capacity needed to meet each agency's requirements (chapter 5). Accordingly, it is assumed that within each option, efficient use is made by PSAs of available capacity.

Four options have been evaluated

The Commission has evaluated four specific options (and variants thereof) for delivering a PSMB capability in areas of Australia where there is existing commercial mobile coverage (table 6.1). It is assumed that PSMB is rolled out nationally, although the implications of taking a state-by-state approach have also been considered.

Table 6.1 **Overview of PSMB delivery options evaluated**
Areas within commercial mobile carrier coverage footprints

	Dedicated spectrum for PSAs	*Coverage in dense urban, urban and suburban areas*	*Coverage in rural and remote areas*	*Number of networks involved*
Option 1 (dedicated)	Yes	Dedicated	Dedicated	1
Option 2a (hybrid)	Yes	Dedicated and commercial	Dedicated and commercial	1
Option 2b (hybrid)	Yes	Dedicated and commercial	Dedicated and commercial	2
Option 2c (hybrid)	Yes	Dedicated and commercial	Dedicated and commercial	3
Option 3a (hybrid)	Yes	Dedicated and commercial	Commercial	1
Option 3b (hybrid)	Yes	Dedicated and commercial	Commercial	2
Option 3c (hybrid)	Yes	Dedicated and commercial	Commercial	3
Option 4a (commercial)	No	Commercial	Commercial	1
Option 4b (commercial)	No	Commercial	Commercial	2

A dedicated PSMB capability (option 1)

A dedicated PSMB capability would mean that PSAs have access to (and control over) their own PSMB network, using their own parcel of spectrum set aside in the 800 megahertz (MHz) band for a PSMB capability on a national basis (box 6.1).

While it is assumed that existing sites and backhaul transmission would be used as part of this option, significant new investment would be required. This includes new base stations, base station equipment, backhaul links and core networks.

PSAs would not be able to ‘overflow’ onto commercial networks for public safety grade mobile broadband services under this option. However, they would be able to purchase standard commercial mobile services, as they do today.

Box 6.1 Spectrum band assumed for the quantitative analysis

There is ongoing debate about the relative merits of different bands of spectrum for a PSMB capability. Specifically, various parties have argued for an allocation of spectrum in the 700 MHz band, whereas spectrum notionally set aside for PSAs by the Australian Communications and Media Authority was in the 800 MHz band (appendix B). Spectrum allocation decisions are the responsibility of the Authority.

For the purposes of quantitative evaluation, the Commission has assumed that any spectrum allocated for a PSMB capability would be in the 800 MHz band. However, the Commission has not evaluated the relative merits of different spectrum bands and thus is not making any specific recommendation on the type or size of spectrum band.

A commercial option (option 4)

A commercial option would mean that PSAs obtain PSMB services from one or more of the mobile carriers through a contract for service. Carriers would determine how best to meet PSA requirements using their own mobile networks and spectrum holdings.

This option would require that mobile carriers 'harden' their networks to improve network reliability. This could include installation of additional battery backup, physical site upgrades and new backhaul links. Adding PSA traffic to mobile carrier networks would also be expected to 'bring forward' investments in sites, spectrum and backhaul.

A commercial option could involve one or multiple mobile carriers. Both possibilities have been evaluated.

A full coverage hybrid option (option 2)

A full coverage hybrid option would provide PSAs with a dedicated network that covers the entire mobile carrier footprint (as per the dedicated option), and their own parcel of spectrum. PSAs would also be able to use one or more of the mobile carrier networks to access additional 'public safety grade' network capacity on a preferential basis.

What is implied by a 'dedicated network' under this option can vary. On the one hand, PSAs could rely on the core network (control centre) of a mobile carrier (that is, the core network is shared). However, the parcel of spectrum set aside for PSAs under this option would *not* be shared, meaning PSAs would still have access to their own dedicated 'channel'. This would be sufficient for some (but not all) of PSAs' capacity needs.

Alternatively, the dedicated network could be supported by a separate core network built for PSMB, which would interface with one or more mobile carrier networks. The potential advantage of a separate core network is that it would provide PSAs with more control over the configuration and operation of the dedicated network. For example, relative to sharing a core network, this option may be more amenable to PSAs (or an agent on their behalf) directly managing the prioritisation of PSA users in real time.

Both alternatives have been considered as part of the Commission's analysis, as has the option of relying on multiple mobile carriers to deliver the commercial component of the capability. Specifically:

- **option 2a** involves use of a single mobile carrier core network, and the shared use of carrier backhaul transmission capacity (managed by the carrier)
- **option 2b** involves a new core network for PSMB plus one existing mobile carrier network, and leasing carrier backhaul for the dedicated network element
- **option 2c** involves a new core network for PSMB plus two existing mobile carrier networks, and leasing carrier backhaul for the dedicated network element.

A partial coverage hybrid option (option 3)

A partial coverage hybrid option would provide PSAs with a dedicated network element that covers metropolitan areas only (defined as areas within the dense urban, urban and suburban geotypes — which cover around 80 per cent of the population), and their own parcel of spectrum.

PSAs would rely on mobile carrier networks for some of their capacity needs in metropolitan areas (once they exhaust their own dedicated capacity). Outside of the metropolitan region, PSAs would rely on mobile carriers for both coverage and capacity.

As with the full coverage hybrid option, PSAs could rely on the core network of a single mobile carrier, or could establish a separate core network built for PSMB, which would interface with one or more mobile carrier networks. Both alternatives have been considered as part of the Commission's analysis. Specifically:

- **option 3a** involves use of a single mobile carrier core network, and the shared use of carrier backhaul transmission capacity (managed by the carrier)
- **option 3b** involves a new core network for PSMB plus one existing mobile carrier network, and leasing carrier backhaul for the dedicated network element
- **option 3c** involves a new core network for PSMB plus two existing mobile carrier networks, and leasing carrier backhaul for the dedicated network element.

Assumptions on backhaul are a key differentiator between hybrids

To illustrate the importance of assumptions about backhaul to the quantitative results, it has been assumed that:

- options 2a and 3a involve PSAs sharing a mobile carrier's backhaul transmission capacity network (as part of a managed end-to-end service that uses the carrier's core network)
- options 2b/3b and 2c/3c involve PSAs leasing separate backhaul capacity to carry data between the dedicated network and a state and territory (hereon 'state'), or PSA, owned and controlled core network.

In practice, different combinations of hybrids are possible. For example, it may be possible for PSAs to more extensively share backhaul capacity with mobile carriers even where they retain their own core network. Further, hybrid options could potentially involve greater efficiencies at the site level in terms of the deployment of new base station equipment.

The Commission is seeking further feedback on the assumptions underpinning the hybrid options for the final report.

6.2 Evaluation of costs

The two main sources of costs considered in this study are the direct network-related costs of delivering a PSMB capability, and the potential indirect costs imposed on other (non-PSA) users.

The approach to estimating direct network costs

Network-related costs can be grouped into four key elements — those associated with the radio access network, backhaul, core network and spectrum (chapter 5). Handset costs have also been included in the analysis (but do not differ across options).

Key network costs have been evaluated quantitatively using a fit-for-purpose, bottom-up approach (box 6.2). The analysis covers a 20-year period (from 2018 to 2037 inclusive) and is national in scope. To allow for comparisons, the cost of providing PSMB under each option is discounted to present value terms (using a real discount rate of 7 per cent).

The cost analysis is premised on estimating the incremental (rather than total) costs of delivering a PSMB capability — that is, the costs associated with delivering PSMB relative to the status quo. These costs are intended to reflect opportunity costs — that is, the value of the next best alternative use of the resources.

This bottom-up costing approach has been applied consistently across options. The Commission is cognisant that there are other ways to estimate the costs of a commercial option, such as using PSA end-user prices. In practice, the prices that a government or PSA might pay for PSMB could differ from the underlying costs of providing the service. This could be due to a number of reasons, including the inclusion of profit margins or the extent of competition in the market (Access Economics 2010). Nevertheless, the lack of a fully functioning public safety grade mobile broadband service in other countries (and a corresponding absence of prices associated with this) makes it problematic to estimate the costs of delivering a PSMB capability using a price-based approach.

Box 6.2 A 'fit-for-purpose' approach to evaluating network costs

The objective of the quantitative evaluation is twofold — to identify indicative cost differences between options for delivering a PSMB capability, and to gain an understanding of key cost drivers. The choice of framework and methodology has been driven by its suitability for these purposes.

The bottom-up approach to estimating network costs involves three key steps:

- geotyping — using census data to assign different geographical areas of Australia to particular geotypes (dense urban, urban, suburban, rural or remote)
- radio access network dimensioning — estimating the number of mobile sites, and other additional network infrastructure, required to meet the coverage and capacity requirements embodied in the PSMB scenarios (chapter 4)
- network costing — applying benchmark cost values (such as the costs of mobile base station equipment) to calculate relevant capital and operating costs.

The key output from the quantitative evaluation is a net present value for each option, assuming a 20-year time horizon. Importantly, the analysis is not designed to:

- produce precise estimates of the total costs of individual options, or individual cost components (some cost items have been excluded from the quantitative analysis as explained in section C.9 of appendix C). Rather, the focus is on relativities
- describe what the architecture of a PSMB network would look like in practice
- identify (in an exact way) the optimal mix of inputs for delivering a PSMB capability.

PSMB service standards

To compare network costs on an even keel, it is assumed that each option would deliver the same level of PSMB network capacity, as defined by the Commission's capacity scenarios (chapter 4). Dealing with the quality dimension of a PSMB capability is more difficult. While the Commission has proposed a starting-point definition of mission critical mobile data standards, the options evaluated in this report are not explicitly designed to meet all of these standards. This reflects limited and conflicting evidence as to whether and what technologies and infrastructure could be put in place to achieve the specified outcomes.

Notwithstanding this, certain levels of service quality are implied by the assumptions made in the quantitative analysis, and are common to all options. Specifically, under each option:

- the network has been designed to provide geographical coverage equal to existing commercial networks, which broadly equates to a population coverage in excess of 99 per cent
- some capital investment is made to the core network to provide priority services to PSAs
- it is assumed that a proportion of network sites are subject to some form of hardening, which implies an improvement to network resilience and reliability.

There is a lack of publicly available information to inform some of the key assumptions and parameters used in the quantitative evaluation. In these cases, a preliminary judgment has been made for the draft report, and sensitivity testing has been used to test the robustness of the results. Feedback is sought on the assumptions and parameters used in the quantitative evaluation to inform the final report. Further details of the approach to the quantitative analysis and assumptions are provided in appendix C.

The approach to estimating indirect costs

Some participants have suggested that delivering a PSMB capability could have consequences for the quality of service experienced by other mobile users — in particular, where PSA and non-PSA users share access to the same network under a commercial or hybrid approach.

There are potentially two indirect effects to consider. On the one hand, enhancements to mobile carrier networks to ensure that mobile services are delivered to a public safety standard could improve the quality of service experienced by non-PSA users (a positive spillover). On the other hand, providing PSAs with access and priority guarantees may mean displacing commercial customers, or degrading their quality of service at certain points in time (a negative spillover) (CDMPS et al., sub. 7; NSW Telco Authority, sub. 30).

Estimating the extent of these impacts quantitatively would require an understanding of how users' quality of service would be affected in net terms, the value users place on those changes (assuming no change in prices), and how mobile carriers would likely respond to delivering services to their broader subscriber base. Due to limited information, the Commission was not able to quantify these effects, and has instead considered this issue qualitatively (section 6.3).

Network cost evaluation results

This section highlights some of the key insights that can be drawn from the Commission's quantitative analysis. (Appendix C sets out the results in more detail.) The quantitative analysis has yielded a number of insights about the relative costs of delivering PSMB using different delivery options. However, in many areas the Commission's quantitative analysis has been limited by the paucity of publicly available data, or a lack of clarity or consensus on technical matters.

The quantitative analysis presented in this draft report should therefore be considered preliminary. The Commission is seeking feedback on the methodology, assumptions and inputs used to refine the analysis ahead of the final report.

Moreover, there are factors other than cost to consider when deciding which delivery option to adopt. In particular, the risks associated with alternative options can bear on the relative merits of the options (section 6.3), and benefits (section 6.4).

A commercial option minimises costs

The Commission's quantitative analysis found that deploying a dedicated network is about 2.9 times more costly than relying on commercial networks. Specifically, the estimated net present cost of the dedicated option over 20 years is just over \$6.1 billion, compared to about \$2.1 billion for a commercial option (table 6.2).

The cost difference between the dedicated option and commercial options can be broken down into two key components.

Greater *capital expenditure* or 'new investment' is required in the dedicated option — on spectrum, mobile base station equipment (to operationalise the dedicated spectrum), and a new core network. This reflects the assumption that there are some costs that would not be reincurred under the commercial option where significant investments have already been made (such as to establish a network coverage layer or build core network capability). It also reflects the assumption that mobile carriers have a wide portfolio of spectrum resources (across multiple bands) which provides them with greater flexibility to meet PSA requirements at least cost (chapter 5) — for example, instead of building a new site, or acquiring new spectrum to meet peaks in demand, carriers can draw on these resources to meet demand and delay new investment.

Greater *operating expenditure* would be incurred in the dedicated option, in terms of annual service charges (site leasing and backhaul costs) and network-related operating and maintenance expenditure, compared to a commercial option. This reflects the assumption that mobile carriers are in a stronger position to minimise PSMB operating costs by spreading certain costs (such as those which may not vary greatly with the level of traffic on their network) over a larger number of users compared to a dedicated option. For example, some operating cost expenditures (such as network site maintenance and billing costs) will be largely invariant to the total number of users on the network.

Table 6.2 **Composition of PSMB delivery costs**[a]

Cost item	*Dedicated*	*Hybrid*		*Commercial*	
		Minimum (option 3a)	Maximum (option 2c)[b]	Minimum (option 4a)	Maximum (option 4b)
	$m	$m	$m	$m	$m
Radio access network equipment	1 150	692	1 048	..	..
Hardening	174	164	123	117	92
Core network and add-ons	143	42	1 190	42	84
User equipment	532	532	532	532	532
Mobile carrier network augmentation	..	52	52	251	251
Spectrum	264	224	264	..	..
Operating costs	3 857	2 627	3 989	1 140	1 146
Total cost[c,d]	**6 123**	**4 335**	**7 201**	**2 083**	**2 107**

[a] The quantitative analysis is highly dependent on various assumptions and input values (appendix C). Altering key assumptions would be likely to materially change the results, as demonstrated by the sensitivity analysis (appendix C). [b] This option assumes state-based approaches in which core network infrastructure is duplicated in each state (hence the large cost differential). [c] This represents the sum of all costs considered in the quantitative evaluation. It should not be interpreted as the total costs that would be incurred in actually deploying a particular option. This is because the evaluation is a partial analysis and does not seek to reflect all costs. Cost items explicitly excluded from the quantitative analysis are outlined in appendix C. [d] Figures may not add due to rounding. .. Not applicable.

Source: Productivity Commission estimates.

Previous studies have also found that it would be more costly to deliver a PSMB capability via a dedicated network compared to other options (box 6.3).

The cost difference between commercial and hybrid options narrows as the geographic region covered by the dedicated component decreases, and as the extent of infrastructure sharing between mobile carriers and the PSMB network increases.

However, even the lowest-cost hybrid option considered by the Commission (option 3a) is estimated to be about twice as costly as a commercial option. In this hybrid it is assumed that PSMB would be delivered using a mobile carrier's core network, but public safety officers operating in metropolitan areas (defined as areas within the dense urban, urban and suburban geotypes and covering about 80 per cent of the population) would have access to a dedicated PSMB network (via dedicated PSMB spectrum) to service 80 per cent of their capacity needs. Outside of this, PSMB would be delivered by the mobile carriers, using their infrastructure and spectrum.

Box 6.3 Previous studies which compare PSMB network costs

Some previous studies which have compared the network costs of delivering a PSMB capability under different options have found that a dedicated PSMB network is more costly.

For example, a study by the Federal Communications Commission in the United States found that a dedicated approach would require at least 2.5 times more capital costs than a shared network model. This study also found that use of a partnership model would reduce ongoing capital and operating costs by at least 10 per cent over a 10-year period.

A version of a report by Access Economics publicly released in 2011 referred to the results of a separate study which compared the costs of different delivery options for PSMB (the report was by Gibson Quai AAS Consulting). Access Economics (2010, p. 13) noted that:

> Over a 15 year license term, Gibson Quai-AAS's estimates indicate that, even under the most generous set of assumptions, a commercial arrangement with a carrier would be substantially cheaper than a private network …

Sources: Access Economics (2010); FCC (2010a).

The cost difference between the lowest-cost hybrid and the commercial option is driven predominantly by two factors (figure 6.1). First, there is an assumed need for new capital investment in base station equipment compatible with dedicated PSMB spectrum at each site within the dedicated network footprint (as denoted by radio access network equipment in table 6.2). Second, it is assumed that additional site leasing costs would be incurred for housing new equipment for a dedicated PSMB network at existing sites.

Adding PSAs to mobile carrier networks is not costless

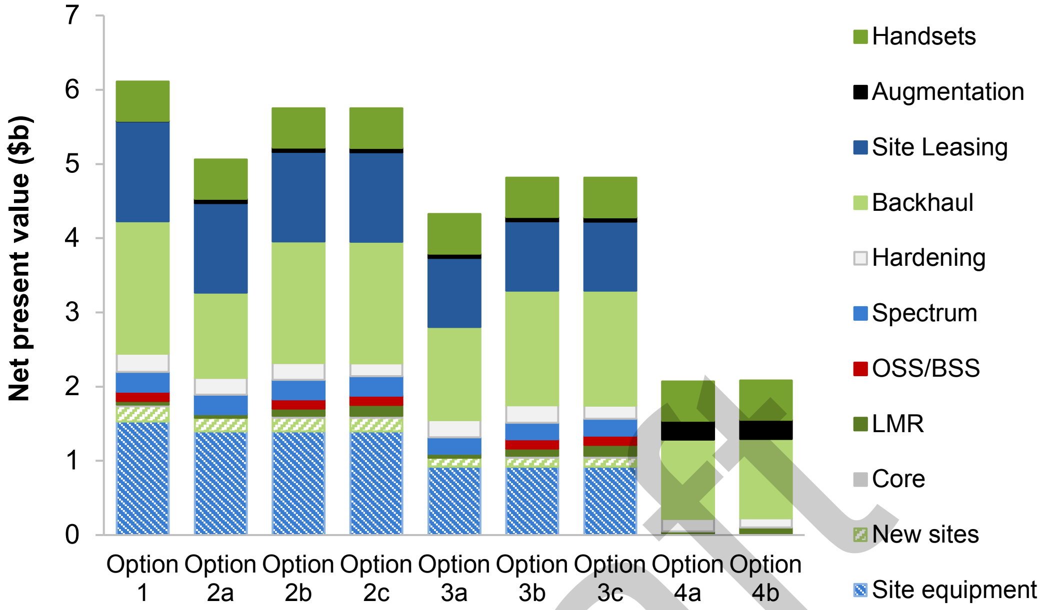
While PSAs may represent a small proportion of a carrier's total customer base, the addition of PSA traffic — which is given a higher priority status than other users — could be expected to impact the investment plans of mobile carriers. Put another way, mobile carriers will incur costs in adding PSAs to their networks under commercial and hybrid options.

It has been assumed that mobile carriers will incur two main types of capital expenditure costs in delivering a PSMB capability:

- upfront investment to harden their mobile networks to provide a level of reliability consistent with delivering public safety grade mobile broadband (chapter 5)
- ongoing investment to add capacity to their networks in order to meet the demands of their broader customer bases (PSAs and non-PSAs included) compared to if they were not delivering PSMB on their networks. This demand could bring forward new site builds or spectrum acquisitions (compared to the status quo) by mobile carriers.

Figure 6.1 **PSMB delivery costs**[a]

By option and cost item[b]



[a] This represents the sum of all costs considered in the quantitative evaluation. It should not be interpreted as the total costs that would be incurred in actually deploying a particular option. This is because the evaluation is a partial analysis and does not seek to reflect all costs. Cost items explicitly excluded from the quantitative analysis are outlined in section C.9 of appendix C. [b] OSS/BSS refers to Operations and Business Support Systems.

Source: Productivity Commission estimates.

Both types of costs are reflected in the quantitative evaluation of commercial and hybrid options and increase the costs of these options. However, because option 4a involves 100 per cent of PSA traffic being carried on a single mobile carrier network, these costs are largest for this option. Further detail on the approach is provided in appendix C.

While these capital expenditure costs are material, the above results indicate that they are significantly less than the ongoing operating costs a mobile carrier(s) would incur in delivering a PSMB capability and meeting public safety grade mobile broadband service levels. For example, incremental capital expenditure is estimated as 42 per cent of total costs over the 20-year period, compared to incremental operating expenditure of 58 per cent. The main components of operating costs that mobile carriers would be assumed to incur include some additional network expenditure (including that related to maintenance of battery backup for resilience purposes) and leasing of additional backhaul to meet PSA requirements.

Differences in hybrid costs depend on assumptions about coverage and the number of mobile networks involved

All other things equal, increasing the size of the dedicated component of a hybrid option increases network costs. This is driven predominantly by the need to deploy additional base station equipment to utilise dedicated PSMB spectrum and other associated site-driven costs which arise from this (including site leasing and site backhaul costs). For example, the cost uplift between options 2 and 3 ranges from about 15 to 19 per cent. Another key way in which hybrid options are differentiated is in how many mobile networks would be involved in delivering the PSMB capability (section 6.1).

Based on the assumptions applied in this study, the quantitative results indicate that the cost of delivering a PSMB capability is between 10 and 31 per cent less costly under option 3a (single mobile carrier network) compared to options 3b and 3c (where multiple networks are involved). This cost difference is predominantly driven by the assumption that option 3a would share existing mobile carrier backhaul to a greater extent.

Tradeoffs to consider between single versus multiple mobile carrier options

Some options considered by the Commission involve multiple mobile networks. In effect, this means PSA users would be able to roam between separate mobile networks — whether between a dedicated and single mobile carrier network (options 2b and 3b), a dedicated and multiple mobile carrier networks (options 2c and 3c) or between multiple mobile carrier networks only (option 4b). This section focuses on the merits of a single mobile carrier option (3a, 3b, 2a, 2b, 4a) or multiple mobile carrier options (2c, 3c, 4b).

There are two effects to consider in comparing single versus multiple mobile carrier options for delivering PSMB (chapter 5). On the one hand, use of multiple mobile carrier networks would add additional network costs — such as where each participating carrier would need to upgrade its core network to deliver priority services to PSAs and to facilitate roaming across multiple mobile carrier networks (with the costs and complexities being higher if roaming was intended to be seamless).

On the other hand, access to multiple mobile carrier networks may provide PSAs with greater depth of coverage and a higher degree of communication redundancy, since they would be able to switch networks in the event one was not available. Given that the purpose of network hardening is to improve network resilience and redundancy, this could, in turn, lower the amount of initial investment needed to harden mobile carrier networks to deliver the desired level of reliability. (That said, in some scenarios, access to multiple mobile carrier networks in the same location might not guarantee greater reliability, such as when a flood or fire takes out all surrounding sites.)

Whether a multiple mobile carrier approach is more cost effective would depend on which of these two effects was more material. For the quantitative evaluation, both of these effects were accounted for by making assumptions about:

- the costs of additional network equipment that might be required to implement a multiple mobile carrier option, such as land mobile radio gateways required to facilitate roaming between PSA narrowband networks and a PSMB network
- the amount of hardening required under each option — a multiple mobile carrier approach was assumed to require battery backup at fewer sites than in a single mobile carrier option (75 per cent of sites compared to all sites).

Based on the approach adopted, the quantitative analysis indicates that the potential cost savings of having a multiple mobile carrier approach in place are outweighed by the additional core network costs (including those to facilitate roaming). However, this result is very much dependent on the assumptions applied.

Due to limited information, the Commission's approach to quantifying these effects between hybrid options is illustrative, and should not be interpreted as a final view of the relative merits of single or multiple mobile carrier approaches.

A national approach for a dedicated network has materially lower costs

If a dedicated option was pursued, the quantitative evaluation indicates that a national approach has the potential to lower costs relative to a state-by-state rollout by eliminating the duplication of core network infrastructure. The quantitative results suggest that a state-based approach — in which separate core networks would be deployed in each state — would be in the order of 1.25 to 1.3 times more costly than a dedicated national approach (with a single core network shared by jurisdictions).

A national approach could also allow for greater exploitation of economies of scale in the procurement of handsets and other end-user devices, particularly if PSAs seek to purchase customised equipment. However, this particular aspect was not quantitatively evaluated due to a lack of available evidence and data on the materiality of these cost differences.

Sensitivity analysis

The quantitative results discussed above are based on some key cost drivers, which in turn are based on a number of assumptions and inputs about how these cost drivers apply across options. These can be described as the 'central case' assumptions.

However, as noted elsewhere in this report, an issue with the quantitative evaluation has been a lack of detailed information and data, and there is a considerable degree of uncertainty around many inputs and parameters. Therefore, an important consideration is whether the results (and in particular, the cost ranking of options) are robust to alternative assumptions and inputs. To assess this, the Commission undertook a partial sensitivity analysis, in which parameters were assigned a lower and an upper bound. To estimate representative 'best' and 'worst' case scenarios, a simulation was undertaken in which several parameters were varied simultaneously in the same manner — all were set to their lower bound or their upper bound.

This section identifies the key insights from the sensitivity analysis — a full exposition is contained in appendix C (section C.8).

Results are highly sensitive to some cost items

Sensitivity analysis suggests that some parameters have only a marginal effect on the estimated costs (such as the opportunity costs of spectrum), and therefore do not affect the cost relativities across options.

On the other hand, the analysis indicates that the results are highly sensitive to several of the assumptions and inputs, with some of these parameters having more bearing on relative costs (table 6.3).

Furthermore, while varying particular parameters may change the cost relativities across options, it does not affect the ranking of options.

Table 6.3 **Sensitivity analysis**
Testing to identify key network cost drivers across all options[a]

Parameter	*Lower-bound effect (relative to base case)*		*Upper-bound effect (relative to base case)*		*Effect on relative costs across different options*
	min. effect[b] (%)	max. effect[b] (%)	min. effect[b] (%)	max. effect[b] (%)	
PSA capacity growth	-2.3	-8.6	5.8	22.1	Medium-high
PSA capacity requirements	-3.9	-14.5	19.5	76.0	High
Site equipment costs	-4.5	-10.7	6.0	14.3	High
Backhaul rental	-5.1	-11.4	5.1	11.4	High
Spectrum allocation	..	..	0	-16.3	High
Operating costs	-1.1	-3.7	2.4	9.0	Low-medium
Discount rate	35.8	40.2	-22.6	-25.1	High

[a] Refer to appendix C for full results of sensitivity analysis, including information on how parameter values were varied. [b] The minimum effect represents the percentage change in costs for the option that is least sensitive to the parameter being tested. The maximum effect represents the percentage change in costs for the option that is most sensitive to the parameter being tested. This is intended to put a range on the impact of different cost drivers on estimated network costs. **..** Not applicable.

Source: Productivity Commission estimates.

Results of best and worst case sensitivity testing

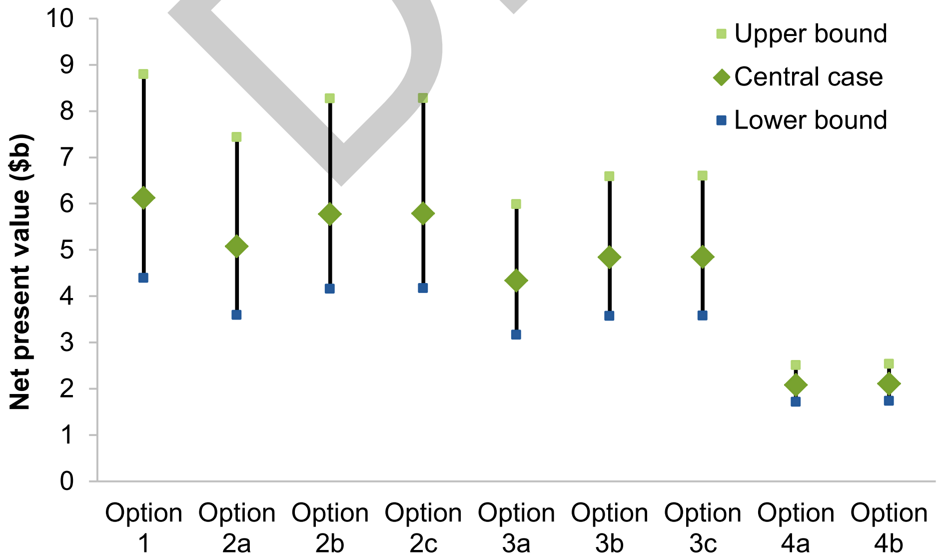
While varying individual parameters one at a time provides context for the importance of those parameters, it does not provide an estimate of the best or worst case outcomes. To do this, the following parameters were varied simultaneously:

- the cost of new sites and site equipment
- backhaul rental costs
- the opportunity costs of spectrum
- site leasing costs
- the amount of spectrum allocated for a dedicated network
- network operating costs (as a percentage of capital costs).

The results suggest that varying key parameters simultaneously has a material effect on estimated costs (figure 6.2). However, the relative ranking of delivery options is unchanged. Moreover, the estimated range of costs for the commercial option is small compared to the other options. Some input values that are only relevant to the dedicated and hybrid options are highly uncertain (such as site leasing and base station equipment costs), and so a wide range of values for these inputs has been considered in the sensitivity analysis.

Figure 6.2 **Sensitivity analysis**

Best and worst case



Source: Productivity Commission estimates.

DRAFT FINDING 6.1

A commercial approach is the most cost-effective way of delivering a PSMB capability to PSAs. Preliminary analysis indicates that a dedicated network is nearly 3 times more expensive than a commercial option.

A hybrid option is also more expensive than a commercial option, though the cost difference narrows as the size of the dedicated network component of the hybrid decreases.

6.3 Evaluation of risks

All infrastructure and service delivery projects involve risks. Risk can be defined as any uncertain but quantifiable consequence of an activity, be it in terms of costs or benefits.[2] Risks can be project-specific (such as technology risks), sector-specific (such as regulatory risks) or economywide (such as inflation risk), and can change over time. These risks can have implications for the costs and benefits of different delivery options for PSMB. This will depend on the likelihood that a risk will occur, and the consequences if it does. While some of these risks can be reduced or avoided, residual risks can remain. (Chapter 7 discusses the role of risk allocation in risk management.)

Some risks differ between PSMB options

Some risks associated with delivering PSMB will vary little between delivery options — for example, the risk that suitable applications will not be developed applies to dedicated, commercial and hybrid options. Other risks could vary in a material way depending on the delivery option. This latter category of risks is the focus of this section.

Participants have raised a number of issues which indicate that different options will involve different risk factors. These have been categorised as:

- technical risks — for example, risks relating to whether the capability meets PSA service requirements, or whether new technology is integrated over time (ARCIA, sub. 2; CDMPS et al., sub. 7; Motorola, sub. 12; Telstra, sub. 19)
- commercial risks — for example, risks associated with PSAs being locked into a specific supplier, or difficulties with contracting (ARCIA, sub. 2; ATF, sub. 4; CDMPS et al., sub. 7; NSW Telco Authority, sub. 30; VHA, sub. 11)
- third-party risks — for example, the risk of adverse impacts on non-PSA users arising from disruption in the quality of service they receive over mobile networks, or due to

[2] By contrast, uncertainty is where it is practically impossible to assign a probability to a particular outcome (Chan et al. 2009a).

reduced competition in the mobile market (ARCIA, sub. 2; Ericsson, sub. 10; VHA, sub. 11).

Risks have been considered qualitatively

Ideally, a cost–benefit analysis would assess costs and benefits using expected values (a probability-weighted average of all possible values) or certainty-equivalent values (OBPR 2014a; PC 2014b). However, there is insufficient empirical information available, both in the literature and from participants, for the Commission to analyse risks quantitatively. Such a task would require a detailed understanding of each risk factor, the probability the risk will be realised, and how it would manifest differently across PSMB delivery options. As such, the Commission has opted to deal with the evaluation of risks in this study in a qualitative discussion of key risks that might differ across PSMB options.

Technical risks

Priority access without dedicated PSMB spectrum has not been demonstrated

Concerns have been raised by some participants that a solution that does not have dedicated spectrum for PSAs will not be able to provide PSAs with guaranteed network access and sufficient capacity during periods of extreme congestion (ACT Emergency Services Agency, sub. 25; MFB, sub. 6; NSW Telco Authority, sub 30; Victorian Government, sub. 28). Some participants have expressed reservations about the ability and willingness of mobile carriers to meet PSAs service requirements (Alcatel-Lucent, sub. 15; NSW Telco Authority, sub. 30).

However, equipment vendors and technical experts have indicated that LTE networks are technically capable of providing priority access and priority services to PSAs (chapter 5), even when sharing spectrum on commercial networks. Individually, elements of prioritisation technology for emergency services on mobile carrier networks are already in place (for example, priority services for Triple Zero calls) or have been demonstrated on a pilot basis (for example, access technology in Telstra’s LANES product). However, the technology has not yet been deployed for PSMB.

In the Commission’s view, it appears to be technically feasible to use LTE networks to provide priority access for PSAs without dedicated spectrum. However, the capability of using the technology in this manner has not been demonstrated in its entirety. Further trials could provide an opportunity to overcome this uncertainty (chapter 7).

There is some uncertainty about whether LTE standards support all elements of dynamic prioritisation

Participants have indicated that one of the desired features of a PSMB capability is that PSAs would be able to have direct control over the capability, including the ability to make adjustments to priority settings in real time (dynamic prioritisation). Concerns have been raised about whether this feature would be possible in the commercial option, and further, whether current LTE standards support this (chapter 5).

The Commission has sought further information on this issue from participants, and will further consider this issue for the final report (chapter 5).

A dedicated network may be at greater risk of delay

Any delay in the rollout of PSMB (beyond the scheduled commencement date) could reduce its benefits (as they will also be delayed). Delay risks are likely to be higher under the dedicated and hybrid options because:

- spectrum availability may have to wait until a formal spectrum allocation decision is made by the ACMA (chapter 5). This process may also be dependent on ongoing international processes to agree on harmonised spectrum for PSMB
- these options require significantly more upfront capital investment relative to commercial options, and there is evidence that lengthy, complex projects are more likely to overrun their expected delivery dates than projects involving less new infrastructure and investment (PC 2014b; Shrestha, Burns and Shields 2013).

Commercial options may be less susceptible to technological obsolescence

Commercial mobile networks are continually upgraded as mobile carriers make new investments to keep up with evolving technology and competitor offerings (Ericsson, sub. 10. Optus, sub. 18; Telstra, sub. 19). Some of these upgrades have high fixed costs that are largely independent of the number of users on the network (for example, rolling out the coverage layer for an updated mobile network technology standard, such as LTE).

Mobile carriers operate multiple technologies, have large portfolios of spectrum and have large user bases (millions of subscribers) over which to recover the costs of new investments (chapter 5). By contrast, a dedicated network option would likely be more constrained in mobile broadband compatible spectrum, and would have significantly fewer users than commercial networks. In addition, some participants have argued that government funding constraints could limit scope for large capital upgrades (BAI, sub. 1).

For these reasons, future technology upgrades (such as 5G technology) on a dedicated network may fail to realise the same economies of scale and scope as a commercial option (or a hybrid option, depending on its design), leading to high per-user upgrade costs. This creates a risk that a dedicated network option (or the dedicated component of a hybrid option) would not be able to incorporate new technologies as quickly, thus leading it to lag technologically behind the service capability available on commercial networks. In turn, this may create risks that parts of the PSMB network cannot take full advantage of new technology, applications and devices developed for consumer markets.

Commercial risks

A commercial approach is more susceptible to supplier lock-in

Supplier lock-in occurs when a customer is dependent on a single (or very few) supplier for a service and is unable to change supplier without incurring significant costs (chapter 7). There are international examples of supplier lock-in influencing future investment decisions in public safety communications networks (box 6.4).

Supplier lock-in can arise in two ways: as a result of a supplier using non-standardised technology (for example, when there is only one supplier of proprietary equipment) or as a result of significant and unrecoverable investments being sunk into a single supplier, which makes it more difficult to change to an alternative provider at a later date (VHA, sub. 11; Victorian Government, sub. 28).

In principle, the use of open standards-based solutions for mobile base station equipment, backhaul and end-user devices means that the risks of supplier lock-in due to proprietary technology would be low under any PSMB delivery option (NEC, sub. 5) — and, in particular, lower than the risks of lock-in with land mobile radio technology (chapter 2). However, any PSMB arrangement that requires significant investment in a single mobile carrier's network (such as a hybrid or commercial option where a single mobile carrier upgrades its core network or undertakes extensive site hardening) represents a sunk investment that may have to be reincurred should PSAs wish to switch suppliers in the future, even if open technical standards are used (VHA, sub. 11). This places PSAs at risk of lock-in due to unrecoverable investments.

Knowledge that switching suppliers would result in some of these 'sunk' costs being reincurred can influence the pricing behaviour of an incumbent supplier, as evidenced in the United Kingdom (box 6.4). Similar pricing incentives could prevail once a PSMB network has been built — for example, if a PSA or state government considers that it has only one realistic choice of supplier for continued PSMB services, which would likely raise the costs of extending the service or procuring new network features (Victorian Government, sub. 28). The NSW Telco Authority (sub. 30) sees this risk as particularly acute if the commercial provider also has control over any dedicated spectrum used by PSAs.

There are strategies available to governments to avoid becoming locked-in — such as public ownership of assets or aligning the length of contracts with the economic life of assets — which can be applied to all delivery options (chapter 7). Spectrum is one key asset that could remain government owned and be reused with another supplier (NSW Telco Authority, sub. 30). However, in a commercial or hybrid option, public ownership may be difficult to apply further, as it is implausible for investments in mobile carrier networks (such as network hardening and core upgrades) to be owned by or transferred to state governments. There may be greater scope to align a commercial contract's length with asset lives, however, because of the wide mix of assets used (with diverse asset lives) and the potential to stagger investments in network infrastructure over time. The extent to which this can effectively mitigate lock-in is unclear.

Box 6.4 **Supplier lock-in and Airwave UK**

Airwave is the current provider of the TETRA land radio system used by police forces and other emergency personnel in the United Kingdom. The Airwave network is commercially owned (including spectrum) with the UK Government contracting with Airwave to acquire services. The cost of this network to government has been much higher than anticipated.

The original estimate was a core service charge of £1.18 billion over 19 years, in monthly instalments, plus £290 million over 19 years for optional services. While total service charges to date are not available, annual reports show that the UK Government paid almost £500 million over the period 2010–2012 alone. This figure does not include £80–100 million per year in charges for other services (such as data and cellular calls) that are made separate to the Airwave network.

In part, the cost increases have been a result of unforseen service additions (such as extensions into the London Underground) that were not envisaged at the time the original contract was signed. Further, usage has been well above expectations, resulting in expensive penalty charges for calls exceeding the pre-arranged limit. There have been reports of police officers being ordered to send text messages rather than use the Airwave network for routine voice calls.

Sources: Delgado (2010); NSW Telco Authority (sub. 30); SCF Associates (2014); UKNAO (2002).

In addition, options which use multiple mobile carriers for service delivery can potentially allow investments to be spread over multiple networks. This may lower the risk of lock-in by reducing the amount of investment sunk into any one network, improving contestability for future PSMB contracts and upgrades (NSW Telco Authority, sub. 30; VHA, sub. 11).

Handset costs could differ across options

End-user devices are compatible with a finite range of frequencies, and manufacturers typically design their devices to be compatible with international standards and frequencies used in consumer markets around the world. Under a commercial option, there would be scope for PSAs to use 'off the shelf' devices (such as consumer handsets) that are already compatible with the spectrum used on mobile carrier networks. By contrast, scope to do this would be more limited under a dedicated PSMB approach if the spectrum band on the dedicated network is not widely supported by device manufacturers, and equipment needs to be customised to meet the needs of Australian PSAs — with consequently higher costs.

These costs could persist over time to the extent that PSAs become locked in to using a spectrum band that is not widely supported in other countries.

Harmonisation with frequency bands used for public safety elsewhere in the world is also a relevant consideration. PSAs may require specialised devices that are tailored to public safety applications and uses (such as 'ruggedised' devices). However, the unit costs of these devices will be influenced by the scale of the global market. Work is currently underway at an international level to harmonise spectrum bands used for PSMB across the Asia–Pacific region (appendix B). For specialised PSA devices, there could be a greater risk that customisation is required under a commercial option (where spectrum bands do not match those used for public safety in other countries) than under a dedicated approach (where there may be greater alignment).

The above challenges are likely to be greatest under a hybrid option. End-user devices in such an option would need to be compatible with the spectrum used on one or more commercial networks in addition to the spectrum used over a dedicated network. Depending on the specific frequency bands used on each network, this would heighten the risk that 'off the shelf' devices are not readily available (either on global consumer or public safety markets) and need to be customised for Australian PSAs.

Multiple mobile carrier options have potential benefits but also risks

Participants have indicated that options for delivering PSMB which utilise the networks of multiple mobile carriers have various benefits (chapter 5) — including providing greater redundancy in case one network is unavailable (therefore, lowering required hardening costs), reducing the risks of supplier lock-in, and generating broader competition benefits in the mobile sector (discussed below).

On the other hand, options which involve PSAs roaming across multiple networks while retaining preferential access (either across multiple mobile carrier networks, or between a separate dedicated PSMB network and a carrier network) could introduce risks to the 'seamless' user experience of PSAs (Telstra, sub. 19). However, participants have indicated that it is technically possible to build in a roaming functionality to an LTE PSMB capability across multiple mobile carrier networks (VHA, sub. 11), and to provide service continuity (Ericsson, sub. 26).

While roaming is technically possible, the implementation of a 'seamless' roaming capability for PSAs across multiple mobile carrier networks (if sought by PSAs) could be operationally and contractually challenging to put in place — especially getting agreement on service levels for when and how roaming will occur, changes to each participating mobile carrier network's software configuration, and billing arrangements (among other things). Roaming agreements are rare in Australia, suggesting that there may be significant commercial and coordination barriers involved. Some participants have expressed a view that the potential impact of roaming arrangements on the commercial operators makes it unlikely that mobile carriers will be willing to support roaming at a reasonable cost (NSW Telco Authority, sub. 30).

There is also a potential risk that pursuit of a multiple mobile carrier option could add to the costs and time taken to put a PSMB capability in place. Contracting and tendering for large procurements can also be costly and time consuming — negotiations between stakeholders need to be undertaken, service levels defined and bids developed. All options for delivering a PSMB capability will require cooperation and coordination between multiple parties — be it within or across governments, and with the private sector. However, the chance of stakeholders not reaching agreement or the tendering process failing potentially increases when greater cooperation and consensus is required between multiple parties (such as across all governments or between multiple mobile carriers), particularly where those parties have conflicting objectives (Mnookin 2003).

Third-party risks

Non-PSA users may experience changes to their quality of service

Delivery of a PSMB capability via commercial or hybrid options could have positive or negative spillovers for non-PSA users of mobile broadband networks.

On the positive side, network hardening undertaken by a mobile carrier to meet higher levels of reliability could also benefit its non-PSA customers. In addition, increased capacity investment over time by a mobile carrier could also benefit its non-PSA customers during periods where PSAs are not using the capability intensively (CDMPS et al., sub. 7). This could increase the value that a mobile subscriber derives from their mobile service if this service quality improvement was not fully captured in revised consumer prices.

On the negative side, access and priority guarantees granted to PSAs that displace commercial customers or degrade their quality of service during certain periods of time would be disruptive for these consumers, and may have flow on negative implications for the community more broadly. For example, negative spillover effects on non-PSA users have the potential to be particularly acute during disasters or busy periods (such as New Year’s Eve) when mobile networks are already heavily congested. It has been suggested that reducing the public’s access to mobile carrier networks during emergencies could result in valuable information that would have been uploaded and disseminated via social media (such as photos and videos) being unavailable (NSW Telco Authority, sub. 30). This could impact on the situational awareness of both PSAs and the broader public.

The decisions taken by mobile carriers in delivering a PSMB capability would largely determine whether the positive or negative effects are more significant. On the one hand, mobile carriers can be expected to have strong incentives not to degrade the quality of service offered to their non-PSA subscribers (including due to risk of customer churn) and would likely carefully manage the impact of delivering PSMB on their networks over time.

On the other hand, rather than add capacity to the entire network and maintain quality of service during these unplanned incidents, mobile carriers might allow a temporary reduction in service levels to commercial customers located in the immediate area. The costs of doing this (for example, through compensation to non-PSA users, or via non-PSA users switching to other carriers) could be less than adding additional permanent capacity. If the price PSAs pay for capacity during unplanned events reflects this lower cost, then PSMB usage will be higher under commercial and hybrid options compared to a dedicated network. This combination of lower costs and increased usage during unplanned events will add up to higher net benefits over time.

In sum, the net result on quality of service for non-PSA users from an approach which involves them sharing network capacity with PSAs is uncertain, as is the value non-PSA users would place on any impacts. How these spillover effects would vary across the commercial and hybrid delivery options is also uncertain. That said, these spillover effects would likely be reflected in the prices charged by mobile carriers (to both PSA and non-PSA users), and mobile carriers could be expected to seek to minimise any adverse impacts on their other customers.

The PSMB delivery option may impact (positively or negatively) on competition

Some participants argued that the PSMB delivery approach chosen could impact on the competitive dynamics in the broader mobile market, positively or negatively.

On the negative side, some participants noted that the degree and level of competition in the commercial mobile market is already less than desirable to deliver competitive outcomes for a PSMB capability, and that Telstra has a coverage advantage over other mobile carriers (VHA, sub. 11; Victorian Government, sub. 28). Participants also expressed concern that any public funding directed towards improving mobile coverage in 'thin' rural markets for PSMB will lead to improvements in Telstra's mobile network (either by extending coverage or increasing quality of service), which would further entrench its position in the market (VHA, sub. 11; Victorian Government, sub. 28).

On the positive side, some participants view the approach to PSMB policy as an opportunity to promote deeper competition in the mobile market more broadly, particularly in 'marginal' regional areas where natural monopoly characteristics mean there is only ever likely to be one network operator (Victorian Government, sub. 28).

Participants put forward various mechanisms for facilitating contestable and competitively priced service offerings for PSMB, and to promote competition in the broader market (which are discussed in greater detail in chapter 7). These include:

- the design of procurement mechanisms to encourage greater competitive tension by bidders (Alcatel-Lucent, sub. 15; NEC, sub. 5; NSW Telco Authority, sub. 30; Rivada Networks, sub. 9; VHA sub. 11; Victorian Government, sub. 28)

- the use of regulation to deliver more competitive regional mobile telecommunications service outcomes, or to ensure there is a sufficient regulatory framework that underpins priority access, quality of service and network arrangements for PSMB delivered over commercial networks (NSW Telco Authority, sub. 30; Optus, sub. 18; PFA, sub. 8; Victorian Government, sub. 28)
- aligning PSMB investments with other Australian Government telecommunications programs in order to maximise efficient investment, such as utilising infrastructure built as part of the Mobile Black Spot program and National Broadband Network to support mobile telecommunications investment in regional markets (ARCIA, sub. 2; CDMPS et al., sub. 7; Optus, sub. 18; Victorian Government, sub. 28).

Best-practice policymaking involves identifying a policy problem, setting well-defined objectives and evaluating options for meeting those objectives (chapter 3). There is merit in governments considering how the approach to delivering a PSMB capability will interact with other objectives and policies they have in place — for example, Australian Government schemes that subsidise landline communications and mobile network extensions in regional areas — to ensure that it is consistent with broader policy objectives.

Nevertheless, designing PSMB procurement to achieve a broad range of objectives — in addition to providing mobile broadband to PSAs — potentially introduces a new set of risks that would also need to be evaluated. These include the risks that:

- multiple goals, and a possible loss of transparency between which goal takes precedence, lead to the adoption of higher-cost solutions
- redesigning telecommunications policy through the alignment of existing programs and legislation delays the implementation of a PSMB capability.

These factors need to be adequately weighed up, along with their associated costs and benefits. That said, competition issues in the mobile telecommunications market are likely to be more appropriately addressed directly through existing policy and regulatory mechanisms than indirectly through the design of PSMB procurement. There are several mechanisms already in place for regulation in the telecommunications sector (chapter 7).

DRAFT FINDING 6.2

There is risk and uncertainty associated with delivering a PSMB capability. Relevant risks include:

- technical risk (whether the capability meets PSA service requirements)
- commercial risk (supplier 'lock-in' and difficulties in contracting)
- third-party risk (potential impacts on non-PSA mobile users).

The nature and magnitude of risk varies across PSMB delivery options. For example, the risk of governments becoming locked in to using a single supplier is most pronounced under a commercial approach, while a dedicated network is most susceptible to delays and technological obsolescence.

6.4 Differences in benefits between options

Three main types of benefits are expected to flow from a PSMB capability: improved public safety outcomes (such as lives and property saved and improved officer safety), and cost savings and productivity gains.

There are multiple complexities in quantitatively estimating the benefits flowing from a PSMB capability, including:

- many benefits are non-monetary and will not be reflected in cash flows.
- limited evidence makes it challenging to estimate the value the public places on non-monetary benefits
- there is significant uncertainty as to how a PSMB capability will be used by PSAs (chapter 3).

As such, benefits have not formed part of the quantitative analysis. To facilitate comparison, the delivery options under consideration have been designed to deliver a similar level of capability to PSAs, with the associated benefits not expected to vary markedly. However, there are some features of a PSMB capability that, in practice, cannot be equated across delivery options and will give rise to some variation in benefits. These are discussed qualitatively below.

Benefits will be realised sooner under commercial and hybrid options

A dedicated network is expected to take longer to deploy than commercial and hybrid options (chapter 5), and technological upgrades are expected earlier on commercial networks (section 6.3). All else being equal, it is preferable to realise a given benefit earlier than later. Commercial and hybrid approaches are therefore likely to provide larger benefits by bringing benefits forward, relative to a dedicated option.

Commercial and hybrid options can scale up network capacity in the short term

Demand for PSMB services is highly uncertain and is likely to be influenced by a complex range of factors (chapter 4). Under a dedicated option, there is a hard upper bound on capacity (at least in the short term) as the network is not able to accommodate any PSA demand beyond what it is initially provisioned to meet. Any excess demand beyond this amount will require capacity rationing until such a time that more capacity can be added (either by way of transportable mobile cells or by permanently adding new network capacity).

By contrast, commercial and hybrid options offer scope to scale up capacity as it is needed — a level of flexibility that could provide additional benefits during unplanned incidents.

This might become a particularly important feature if PSMB traffic or capacity turns out to be higher than expected — either in the form of unexpected 'peaks' or due to a higher rate of demand growth.

Reservations about commercial options could delay benefits

Participants have indicated that PSAs have reservations about sharing a network with non-PSA users, or ceding a level of control to a mobile carrier (for example, ARCIA, sub. 2; ATF, sub. 4; PFA, sub. 8).

Previous mission critical communication networks have generally been 'private', that is, built and operated for the exclusive use of PSAs. These networks have, in general, been controlled by PSAs or a government agency acting on their behalf. Commercial networks are a departure from this status quo — they are both shared with the general public and shift the locus of network control away from PSAs and to a private company.

Significant organisational and behavioural change within PSAs — and trust that the technology will work when it needs to — will need to occur before any PSMB capability can be used to its full potential (CDMPS et al., sub. 7; chapter 7). There are various ways that confidence in a PSMB capability could be developed in a way that allows such organisational changes to take place, such as the effective trialling of commercial options (chapter 7).

7 Implementing a PSMB capability

Key points

- State and territory governments can decide whether and how to become involved in providing public safety mobile broadband (PSMB) to their public safety agencies (PSAs). If jurisdictions choose to support PSMB, there would be benefits in creating a statewide implementation agency in each jurisdiction to minimise duplication.
- Jurisdictions will also need to weigh up the costs and benefits of different levels of coverage and quality of service, and set funding arrangements. Prices that reflect the true cost of providing PSMB would encourage PSAs (as users) to seek out the most efficient uses of it.
- Each PSA will need to revise operational procedures and implement training programs for its staff. Ministers in each jurisdiction should facilitate formal protocols between PSAs for sharing information and prioritising users (where a PSMB capability is shared).
- State and territory ministers should also agree on a national set of minimum technical standards to facilitate interoperability across jurisdictions and agencies.
- The Australian Communications and Media Authority is currently considering whether to make spectrum in a specific band available for PSMB. Any administrative allocation of spectrum should be priced at its opportunity cost.
- Contracts negotiated between governments and commercial entities would be a more appropriate way to secure a PSMB capability than regulatory compulsion.
- Value for money should be the primary objective in public procurement. Other policy instruments are likely to offer more effective ways to meet additional government objectives.
- The Australian telecommunications sector poses special challenges for procurement. There is a relatively small number of network operators and equipment suppliers, and some parts of the country are covered by a single network.
- State and territory governments can seek more competitive procurement outcomes by:
  - benchmarking bids against other cost data and making tender processes transparent
  - splitting up tenders by service and/or region to encourage a larger number of bidders
  - negotiating on behalf of their PSAs
  - leveraging their infrastructure and spectrum holdings in negotiations
  - using short-term contracts that require adherence to national technical standards.
- Incremental implementation — where states and territories formally trial a PSMB capability on a small scale before expanding it more broadly — would have considerable value. The timing of PSMB investments will likely differ across jurisdictions depending on their needs.

Even where a public safety mobile broadband (PSMB) capability uses the most efficient combination of inputs, it can still impose large unnecessary costs on the community if it is implemented poorly. This chapter examines how PSMB can be implemented efficiently. It covers institutional and governance arrangements (section 7.1), national coordination and standards (section 7.2), spectrum allocation (section 7.3), the role of regulation (section 7.4), public procurement (section 7.5) and the timing of implementation (section 7.6).

7.1 Institutional and governance arrangements

Institutional and governance arrangements shape how public projects are managed and delivered. These arrangements are most effective when responsibilities are assigned to the parties with the right authority and expertise to undertake them, and when accountability mechanisms give those parties an incentive to fulfil their duties in the interests of the community as a whole. The Commission has previously set out principles that can guide governments in crafting these arrangements (box 7.1).

Box 7.1 Principles for good governance in public infrastructure

Roles and responsibilities are clearly defined

All parties should have clearly defined roles and a clear understanding of their responsibilities. This includes a division of responsibilities between elected governments and entities charged with developing investment plans and delivering infrastructure services.

Ministers are well placed to make decisions about the public interest, set policy objectives and develop policy or regulatory frameworks to guide the functions of delivery entities and regulators. By contrast, decisions related to service provision and applying regulations are better left to institutions that are independent of — but accountable to — governments, to reduce the risk that decisions are politicised. In particular, independent entities are usually better placed to make commercial, investment, procurement and regulatory decisions.

Entities are held accountable for their actions

Public entities (via their boards) that report to ministers can be held accountable for meeting policy objectives and acting in accordance with their requirements. Requiring entities to report publicly on their processes, operations and outcomes can provide a further layer of accountability. Regulatory decisions and ministerial directions should be published.

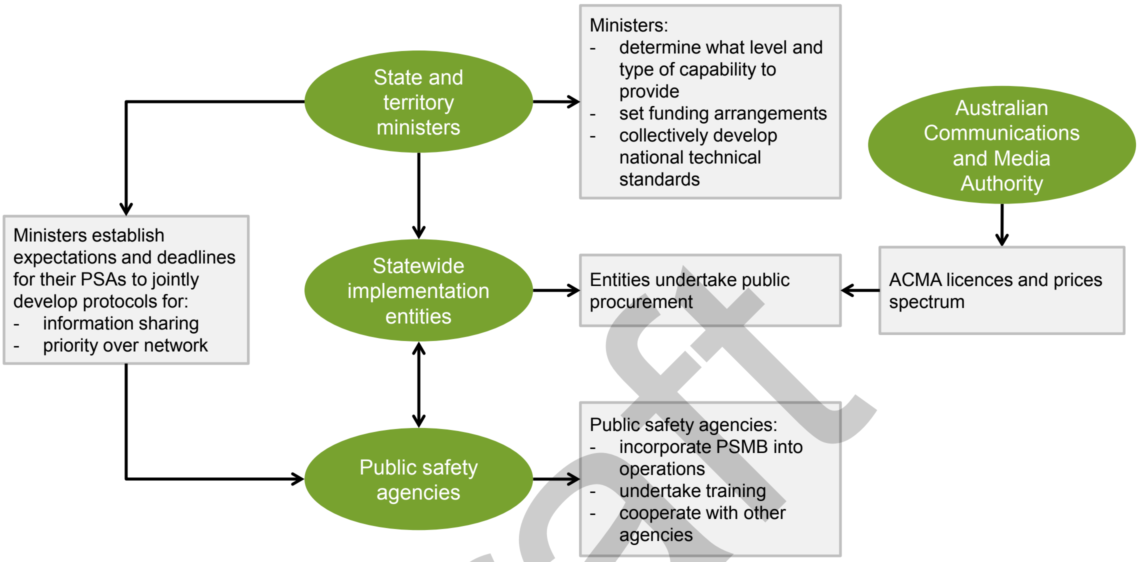
Entities possess sufficient capability to fulfil their responsibilities

Governments need to consider whether each party has the appropriate resources and capability to fulfil its assigned responsibilities (including suitably skilled staff). In practice, this can mean ensuring that infrastructure delivery agencies have sufficient technical and commercial ‘know how’. It can also mean assigning responsibilities to entities that have the most appropriate expertise and authority.

Sources: PC (2011, 2014b).

All jurisdictions and their public safety agencies (PSAs) will have a role to play in implementing a PSMB capability. These roles are summarised in figure 7.1 and discussed throughout this chapter.

Figure 7.1 **Roles and responsibilities for implementing PSMB**



State and territory governments are responsible for PSMB

State and territory governments have primary responsibility for public safety and emergency management (chapter 2). This includes setting policy and funding PSAs to undertake their duties. Accordingly, each state (and its relevant minister(s)) will need to decide if and how it will be involved in the provision of a PSMB capability.

As a first step, each jurisdiction can decide whether to become involved in providing a PSMB capability by 2020, or whether to leave decisions to individual PSAs (either independently or cooperatively).

Some duties are best performed by governments. State government ministers are directly accountable to their communities and so would be best placed to set PSMB policy objectives, timelines and funding arrangements. For example, police and emergency services ministers in each jurisdiction could set clear expectations on what outcomes they expect from a PSMB capability (in terms of improved PSA operations) and over what timeframe this capability should be provided (for example, by 2020). They could also set clear requirements for competitive tendering and public reporting on progress.

Tradeoffs will need to be made

In setting objectives, state and territory governments will need to make tradeoffs between the level and type of capability to provide and the cost involved. In deciding which specific deployment approach to use for PSMB (dedicated, commercial or hybrid), jurisdictions — in consultation with their PSAs — will need to weigh up the costs, benefits and risks of:

- the network capacity and quality of service (including reliability, interoperability and so on) to be delivered to PSAs
- providing a permanent PSMB capability outside of the footprint of commercial mobile carrier networks or relying on other communications options.

This draft report provides a framework for making these tradeoffs, and draws out key drivers of differences across deployment approaches. Ultimately, each jurisdiction will need to make these tradeoffs transparently in deciding on the most suitable course of action to take given its individual circumstances.

In particular, there is a risk of a PSMB capability failing to meet public safety requirements under any deployment approach, and ultimately this risk will fall on governments (section 7.5). In specifying service requirements for a capability, jurisdictions will need to consider how much risk they are willing to bear and articulate this transparently.

Accountability mechanisms are required

Where state governments choose to be involved in implementing PSMB, they will need to establish institutional and governance arrangements in line with good-practice principles (box 7.1). There are technical and commercial decisions that would be best delegated to experts. Jurisdictions could establish a state-owned agency to undertake these duties (or task an existing agency), as set out below.

These implementation agencies will need to be held accountable, both to governments (and the community) and to PSAs. They will also need to consult widely with PSAs on an ongoing basis. One way to facilitate this would be for jurisdictions to appoint representatives from each PSA to the board of the statewide agency.

State and territory governments can further facilitate accountability through putting in place frameworks for monitoring and publicly reporting on PSAs' activities and the outcomes they achieve for the community (such as crime rates or incident response times). Such reporting can help to show how PSAs are using a PSMB capability and the public safety outcomes it is being used to deliver. This can also help governments and the community to weigh up the costs of providing PSMB over time against the benefits being achieved.

However, care is required. Some PSA activities and outcomes are already publicly reported by state governments, including on a national basis through the annual *Report on*

Government Services (SCRGSP 2015). But the indicators currently reported against do not cover all aspects of PSAs' performance, often because it is difficult to accurately measure some outcomes or to link these to the performance of individual PSAs. Ongoing improvements in performance measurement may be needed to improve awareness of how specific PSA activities affect community outcomes, and to reduce biases that can arise where efforts are focused on areas that are measured at the expense of those that are not.

Funding models can facilitate efficient use of PSMB

While state and territory ministers are best placed to make decisions about funding arrangements, individual PSAs are best placed to decide how to use a PSMB capability, just as they are with their other inputs and resources. Jurisdictions can facilitate the efficient use of PSMB (and efficient investment in it over time) by adopting efficient pricing models. In short, this would mean that the prices that PSAs pay for PSMB (for example, from a statewide agency) reflect the cost of delivering the service.

In most markets, consumers of a service are charged in line with their use of it, and this gives them an incentive to use only as much as they are prepared to pay for. It also sends a signal to the service provider about their customers' demand, helping them to make decisions about future investment. When the prices paid reflect the true cost of delivering a service, this leads to allocative efficiency — a situation where resources are directed to their highest-valued uses.

In purchasing PSMB services, PSAs will have to decide what level of capability they are willing to buy and compare the value they get from spending more on PSMB from spending their resources on other priorities or inputs (such as vehicles and equipment). Cost-reflective pricing would effectively encourage PSAs to weigh up the benefits of using PSMB against the costs. It would also give them an incentive to manage their demands on the network, develop new ways to use PSMB in their operations, develop new applications and, ultimately, use PSMB to maximise the outcomes they deliver for the community (box 7.2).

While this approach would in principle be efficient, in practice it may be hard to implement if PSAs have limited capacity to purchase PSMB services (even where this would have net benefits for the community) without displacing other inputs. Where state or territory governments choose to assist PSAs with these additional costs, assistance should be in the form of an increased budget allocation. This would preserve the incentives PSAs have to use PSMB efficiently, relative to alternative funding models (such as directly subsidising the provision of PSMB).

DRAFT FINDING 7.1

Prices that reflect the cost of providing a PSMB capability would encourage PSAs to use it efficiently.

Box 7.2 Prices can encourage efficient use of PSMB

In many markets for infrastructure services (such as electricity, water and transport), prices are used to recoup the costs of investing in and operating infrastructure. This can be done by way of a single fee (which is common in public transport) or a two-part tariff (as often used for urban water). In the latter case, an efficient model is to charge users a flat annual fee (reflecting capital costs) and a per-unit usage charge (reflecting operating costs).

A further model is package pricing (also known as bundling), which has been increasingly adopted by commercial mobile carriers for their business customers. This involves charging a flat per-month fee which covers a bundle of services up to a specified level (for example, a certain amount of data downloads or voice calls). Additional services, or usage above the predefined level, can incur additional charges.

The influence that pricing has on how a PSMB capability is used will depend on the structure of prices and the type of deployment approach. For example, under a fully commercial PSMB capability with per-megabyte billing (above a predefined level of data use), PSAs would need to weigh up the costs of using additional data against the benefits. In a hybrid approach where PSAs can overflow onto commercial networks, they would need to identify when it is worthwhile to overflow, given the prices they would be charged for doing so. And in any arrangement where there are no (or low) usage charges (such as under a dedicated network), PSAs would need to pay for any additional capacity or coverage that is required.

However, PSAs will not always need to pay more to use a PSMB capability when they need it most. They can also take steps to manage their network demands — and will have an incentive to do so in periods when the network is congested or usage charges are high. Options include:

- delaying some business-critical traffic to a later time, or slowing non-urgent traffic down to allow greater capacity for more pressing needs
- prioritising specific public safety officers or applications over the network (with lower priority users given slower speeds)
- moving some traffic on to Wi-Fi systems (and thus off the network)
- downloading non-urgent data (such as video) directly from end-user devices, rather than transmitting these data over the network (‘store and forward’).

Some study participants noted that PSAs will need to actively manage their demands on a PSMB capability, for example, by varying video quality or data transmission speeds at different points in time to best meet operational needs (sometimes known as ‘compression and broadcast’) (CDMPS et al., sub. 7).

There would be benefits in using a statewide implementation agency

Implementing a PSMB capability will involve a number of technical and commercial tasks. These could include:

- developing the technical specifications that a PSMB capability would need to meet (in close consultation with PSAs and in line with requirements set by ministers)
- performing technical analysis and market testing
- directly procuring a PSMB capability

- long-term investment planning
- enforcing technical and operational standards across PSAs to enable interoperability (such as network and software compatibility and information-sharing protocols)
- performing network control tasks and providing day-to-day operational support.

While these tasks could be performed by individual PSAs, in some jurisdictions there would be benefits in establishing a statewide agency to undertake some (or all) of them, in line with policy objectives set by ministers. History suggests that a statewide approach is likely to be more effective than letting each PSA independently make procurement decisions. This has led to duplication of investments in land mobile radio (LMR) networks and significant constraints on technical interoperability across agencies in many jurisdictions (chapter 2). By contrast, a statewide approach would help to minimise duplication of equipment and procurement, and could also lead to economies of scale (for example, where purchasing a larger number of handsets would reduce the unit cost) (Victoria Police, sub. 17).

A statewide approach would also offer opportunities to coordinate PSMB investments with those in LMR networks or other state government programs (such as mobile black spots initiatives). Some jurisdictions have already established dedicated agencies to manage PSA communications and invest in LMR networks at the statewide level (box 7.3), and could potentially task these agencies with the implementation of a PSMB capability.

Some coordination at the state level is therefore likely to be beneficial, though each jurisdiction will need to decide what form this coordination should take. A statewide agency could implement a single PSMB capability that is used by all PSAs, or it could assist individual PSAs to make their own investment decisions.

The risk with a statewide capability is that it does not adequately meet the requirements of each PSA (thereby reducing take-up of the capability and hence its benefits). This was the experience in the United Kingdom, where commercial mobile services were rolled out for police forces without adequate consideration of how the technology would be used or engagement of individual forces (UKNAO 2012).

Such risks are more likely where there is considerable divergence in the needs of individual PSAs, for example, if PSAs are already at different stages of using mobile broadband services, are at different stages of investment in LMR networks, or are not yet ready to invest in PSMB. In these states and territories, a less prescriptive approach may be warranted — for example, statewide agencies providing expertise and coordination, but leaving decisions about the timing of PSMB adoption and other matters to individual PSAs.

Box 7.3 **Public safety communications agencies**

New South Wales

The NSW Telco Authority was established in 2011 to coordinate radio telecommunications policy and services for all NSW Government agencies (including police, fire and ambulance). The Authority is responsible for managing spectrum holdings, procuring and delivering communications technologies, setting technical standards and consolidating government-owned infrastructure to remove unnecessary duplication and costs. It owns and operates the NSW Government Radio Network, with network management and maintenance outsourced to a private-sector provider.

Victoria

The Emergency Services Telecommunications Authority manages the provision of communications for Victoria's emergency services agencies (police, fire, ambulance and the State Emergency Service). This includes procuring and delivering telecommunications services over several networks (the Metropolitan Mobile Radio, Mobile Data Network, Emergency Alerting System and StateNet Mobile Radio) and managing the associated spectrum. The authority also operates the Triple Zero emergency call service in Victoria and dispatches emergency services.

Queensland

The Public Safety Business Agency was established in 2013 to provide strategic and corporate services to Queensland's PSAs. This includes holding and maintaining infrastructure and communication technology assets. The agency has responsibility for the Government Wireless Network, a digital communications network that provides voice and narrowband data services to PSAs.

Sources: ESTA (2014a); NSW Telco Authority (sub. 30; 2014); PSBA (2014).

Individual PSAs will need to adapt

Irrespective of how it is delivered, the benefits of a PSMB capability will depend on *how* PSAs use it (chapter 3). PSAs themselves are best placed to determine how it should be incorporated into their operations. This will require revising operational procedures and protocols, including to manage agency demands on a PSMB capability in peak periods (in line with pricing arrangements, discussed above). It may also require cultural change within PSAs. Agency heads would be well placed to take leadership for these changes.

Making the most of a PSMB capability would also require each PSA to implement education and training programs for its staff (customised to its specific needs and applications) and to invest in developing new applications as technologies continue to develop. This could include finding new ways to use mobile broadband to better deliver public safety outcomes and adapting to changing community expectations about how members of the public can communicate with emergency services (for example, by uploading images and video or communicating over social media) (chapter 3). Efficient pricing models and accountability arrangements, as discussed above, can give PSAs an incentive to make these changes.

Further, PSAs will need to agree on protocols for working together to make the most of PSMB. This process should be led by ministers, as set out below.

Ministers will need to facilitate greater cooperation among PSAs

Interoperability requires more than just compatible technology (figure 7.2). It also needs PSAs to be willing to work together and effectively share information where this would lead to better public safety outcomes — regardless of how a PSMB capability is delivered. Differences in operational procedures (and even terminology) have impeded effective cross-agency collaboration in the past (chapter 2). Indeed, inquiry participants identified non-technological factors as significant barriers to interoperability (for example, Motorola, sub. 12; Victoria Police, sub. 17; Victorian Government, sub. 28).

Figure 7.2 **Elements of interoperability across public safety networks**

Source: Adapted from US Department of Homeland Security (2013).

However, interoperability is not always necessary or even desirable. Agencies sometimes deliberately restrict what information they share with others, such as sensitive criminal information that needs to be tightly controlled (Victoria Police, sub. 17). This also needs to be taken into account as a PSMB capability is adopted.

A PSMB capability would allow much greater information sharing across agencies, including the sharing of new forms of information. Some jurisdictions already have protocols in place for sharing information and coordinating emergency communications, such as Victoria (Victoria Police, sub. 17; Victorian Government, sub. 28). Information-sharing and security protocols may need to be reassessed and amended (or, where they do not exist, created) to make the most of PSMB. These could cover agencies working across state borders as well as with other agencies within the same jurisdiction.

Within each jurisdiction, PSAs will also need to cooperate when they share a common PSMB capability. Many PSAs are used to having their own communications networks, or their own dedicated channels on a shared network (that is, a 'partitioned' network, where each agency has a fixed amount of network capacity). However, this model would generally be an inefficient way to provide a PSMB capability, as it could artificially constrain an agency's ability to scale up its data use during an emergency (chapter 5).

Long Term Evolution (LTE) technologies offer a more flexible approach by potentially allowing specific users and applications to be given a higher priority over a shared network (while also protecting the security of communications) (chapter 5). Implementing prioritisation arrangements would require PSAs to agree on protocols for how their users and applications are to be prioritised over the shared network in specific operational situations. The need for such protocols was recognised by several study participants (box 7.4).

Box 7.4 **Participant views on PSAs sharing a PSMB capability**

There does however need to be protocols developed between the agencies to manage the available capacity. It is likely that once PSMB becomes a reality, there will be latent demand emerging across the emergency services sector which cannot be predicted to any degree of accuracy at this stage. The best scenario is to have the representation and protocols in place to manage capacity issues on an on-going basis. (MFB, sub. 6, p. 15)

The management of competing demands will need to be agreed amongst PSAs and the necessary policies put in place. (Motorola, sub. 12, p. 24)

[R]eaching agreement between agencies as to the application of different priority levels for different agencies is something that will need to be agreed and will be dependent on a strong PSMB governance body able to negotiate these business operating processes. (Ericsson, sub. 10, p. 16)

It is suggested that something like a PSMB Dynamic Capacity Allocation Protocol would need to be developed in conjunction with the customer PSAs and the PSMB Managing Body and PSMB Service Provider(s). This Dynamic Capacity Allocation Protocol would provide a model to assess the severity and potential network impact of escalating incidents, and guide the decisions to reconfigure the PSMB service as necessary to support the PSAs. (Victoria Police, sub. 17, p. 14)

Agreeing on protocols for information sharing and network priorities will be challenging in some jurisdictions. PSAs are unlikely to come to agreement quickly. There is a role for ministers to lead efforts to develop formal inter-agency protocols within their jurisdictions by setting clear expectations and deadlines for when these protocols need to be put in place. This could be done as part of broader processes for inter-agency collaboration on emergency management and public safety that have been put in place over recent years in some jurisdictions.

DRAFT RECOMMENDATION 7.1

If state and territory governments decide to deploy a PSMB capability, police and emergency services ministers in each jurisdiction should set clear expectations and deadlines for PSAs to develop formal inter-agency protocols for:

- sharing information, including security procedures to safeguard sensitive information
- prioritising specific agencies, users, devices and applications, where a PSMB capability is shared among agencies
- specifying responsibility for administering these arrangements and exercising dynamic control over network settings.

The Australian Government has a more limited direct role

The Australian Government (and its agencies) has primary responsibility for the regulation of the telecommunications sector. This includes the regulation and allocation of radiofrequency spectrum (section 7.3) and the economic regulation of telecommunications services and infrastructure (section 7.4).

In addition, the Australian Government directly funds the Australian Federal Police, Australian Maritime Safety Agency and some other PSAs (chapter 2). As with the states, the Australian Government will need to consider whether and how to intervene in implementing a PSMB capability for its PSAs. One option is to fund agencies to procure a PSMB capability, either from the private sector or by purchasing access to state-based PSMB capabilities from each state and territory government. In the latter case, the Australian Government may decide to directly negotiate with other jurisdictions on behalf of its PSAs.

The Australian Government also provides national policy leadership and coordination in some areas. This is delivered through the Department of Communications (with responsibilities covering telecommunications and spectrum policy) and the Attorney-General's Department (with responsibilities in emergency management and national security). Both departments will need to work with state and territory governments to facilitate the implementation of PSMB, including through sharing expertise and addressing any policy barriers to the efficient use of PSMB.

The Australian Government could choose to become more directly involved in the delivery of a PSMB capability within each state and territory if there are national interest considerations. This might involve, for example, seeking to develop common technical or service standards for PSMB, providing funding support, or exercising its regulatory and legislative powers to encourage a particular outcome.

However, direct Australian Government involvement would have risks. Individual states and territories are ultimately responsible (and accountable) for the actions and outcomes of their PSAs — and could effectively veto any attempt by the Australian Government to impose a PSMB capability that does not meet their requirements. The states are also better placed to understand the specific needs of PSAs in their jurisdictions and tailor their policy interventions accordingly.

The Australian Government will have an important role to play in relation to spectrum allocation (section 7.3). Moreover, even though direct intervention in state and territory decisions on PSMB is unlikely to be justified, this would not *preclude* some form of national cooperation led by the states (section 7.2). Likewise, this would not rule out the Australian Government taking a leadership role to encourage adoption of PSMB across states or offering assistance in the development of technical standards.

7.2 National coordination and standards

While each jurisdiction will be primarily responsible for determining whether and how to deliver a PSMB capability, there may be benefits in some form of national coordination. Other federations have already established governance models to coordinate the implementation of PSMB nationally (box 7.5).

National coordination could cover some or all states and territories, but would require the buy in and agreement of all involved. In identifying areas where coordination and/or standardisation should occur, individual jurisdictions will need to consider whether the benefits exceed the costs. Technical standards in some areas could facilitate interoperability (discussed below). However, jurisdictions may prefer to retain flexibility in other aspects of implementation.

A single national PSMB capability could be impractical

Several study participants advocated for a single national PSMB capability — that is, a single service used to provide mobile broadband to PSAs across the country (for example, a national dedicated network or nationwide contract for commercial services). Some argued that this would be necessary for providing interoperability across jurisdictions — for example, by providing the same kind of capability in each state at the same time (ARCIA, sub. 2; BAI, sub. 1; Ericsson, sub. 10; NEC, sub. 5; Telstra, sub. 19).

A national service could also offer cost savings relative to each state adopting a separate capability. As discussed in chapters 5 and 6, a state-by-state approach to deploying a dedicated network could require greater investment in some network components (such as core network equipment) compared to a national model.

However, use of a single national PSMB service across the country could constrain the flexibility of each jurisdiction to implement a solution that best meets its needs at least cost, or at the right time, given its other policy and funding priorities. There is also a risk of delays or cost increases arising from the need to get agreement from all jurisdictions on key design and implementation matters, or from sudden policy changes in any individual state or territory. And, not least, a fully national approach could limit scope for jurisdictions to take different approaches and learn from each other over time (sometimes referred to as 'competitive federalism').

Box 7.5 **PSMB governance models in other federations**

United States

The US Congress established the First Responder Network Authority (FirstNet), a federal agency, in 2012 to deploy a nationwide mobile broadband network for public safety communications. FirstNet holds 20 MHz of dedicated spectrum and will use this to build a dedicated network. It is required to notify the governor of each state how it will construct and operate the network in that state. However, governors can choose to opt out and instead build their own state-based network, provided this meets specific technical requirements in federal legislation. The precise operation of these rules, and the associated spectrum-sharing and funding arrangements, are yet to be fully clarified.

Canada

The Canadian Government has announced that it will allocate 20 MHz of spectrum for public safety use and licence this spectrum to a nonprofit national entity. This entity will not deploy or operate a mobile network itself. Instead, provinces and territories will each establish a regional service delivery entity to deploy a mobile broadband capability, using either the dedicated spectrum, commercial mobile services, or a combination of the two. These regional entities must comply with technical standards set by the national entity to ensure interoperability across provinces/territories and with the United States (in border regions).

Source: Appendix B.

Common technical standards would support national interoperability

Compatible communications technologies are a prerequisite for achieving national interoperability. Even where each jurisdiction takes its own approach towards implementing PSMB, there would be benefits in a set of common technical standards that apply nationally. These would support interoperability between jurisdictions (for example, when public safety officers need to cross state borders) as well as between PSAs within each jurisdiction. Common technical standards were favoured by many study participants (box 7.6).

Box 7.6 Participant views on national standards and governance

Victoria Police's concern is that without a National Governance Structure the opportunity will be lost to truly operate nationally in a joined up manner, and deliver such broadband capabilities within and across 'borders' in an unfettered secure and resilient manner. (Victoria Police, sub. 17, p. 9)

National interoperability needs to be viewed in terms of national governance protocols, common spectrum, compatibility of devices, ability to connect across networks, management of information within jurisdictions, agreed protocols for sharing information. (MFB, sub. 6, p. 10)

The PSMB capability therefore will provide opportunities for national interoperability if agreement can be reached between the States and Territories to the standards to be adopted, the design of their respective networks, and the method of network operation assuming that the PSMB capability will be provided on a network of networks basis. (CDMPS et al., sub. 7, p. 28)

[I]f a national, central forum were established to set the standards, policy frameworks, and user requirements for the nation's emergency services, then agencies would have the ability to coordinate their budget and procurement cycles to take advantage of collective purchasing power for broadband equipment and services. (Motorola, sub. 31, p. 7)

If PSAs build and manage PSMB networks then it may be beneficial to appoint a PSA telco authority to coordinate State/Territory solutions, and to establish a national committee to take responsibility for ensuring interoperability and defining standards and protocols for inter-agency use of the PSMB network. (VHA, sub. 11, p. 7)

While the content of common technical standards is a matter for jurisdictions to agree on, such standards would likely need to cover the following aspects of PSMB to allow for national interoperability:

- technology choice and standards for network equipment and end-user devices (LTE technology based on open international standards developed by the 3rd Generation Partnership Project (3GPP))
- protocols for allowing public safety officers to access PSMB capabilities used in other jurisdictions when required, covering linkages between networks to allow roaming (including billing and payment arrangements)
- the compatibility of end-user devices with the specific spectrum bands used in each jurisdiction (either commercially owned spectrum or PSA-dedicated spectrum)
- backwards compatibility of end-user devices (allowing, for example, public safety officers to operate on another network with less-advanced technology)
- the compatibility of data encryption technologies, software and end-user applications.

Standards in these areas could also help to reduce the need for individual public safety officers to use multiple sets of equipment (for when they cross state borders) and potentially lead to economies of scale in procurement (for example, by reducing the need for handset equipment to be customised differently for each jurisdiction). Aligning these standards with open international standards as far as possible would also improve the ability to achieve competitive procurement outcomes (section 7.5).

However, in setting common standards, jurisdictions will need to consider what level of technical interoperability they are prepared to achieve and how to meet this in the most cost-effective (or least restrictive) way. They will also need to consider how common standards might affect their leverage and flexibility in commercial negotiations (section 7.5) and the relative costs and benefits of attaining interoperability with other jurisdictions.

In particular, some areas may be better left for individual jurisdictions to decide on a case-by-case basis rather than being embedded in common standards. These could include the timing of PSMB investments, the use of particular mobile broadband applications and specific quality-of-service levels. For example, the Government of South Australia (sub. 29, p. 3) submitted that while a national body should develop a governance framework for PSMB, it 'should not provide direct governance of state based PSMB requirements and services, or impose such items as upgrade cycles, technology restrictions and usage levels'. Similarly, the Victorian Government (sub. 28) submitted that only states and territories are in a position to define 'mission critical', and the NSW Telco Authority (sub. 30) contended that responsibility for the design and build of a PSMB capability remains with individual states and territories.

Jurisdictions will thus need to decide whether to implement common standards that go beyond interoperability and cover other areas, such as specific service standards for a PSMB capability. This would be similar to the approach taken in other countries (such as the United States), where national standards have been developed covering network reliability, availability, redundancy and security (appendix B). In particular, the Government of South Australia (sub. 29) submitted that there is a need for a uniform baseline across jurisdictions with regard to mission critical requirements.

In any case, minimum technical standards to support interoperability across Australian jurisdictions would not preclude two or more states or territories from jointly setting standards in other areas (or even jointly implementing a shared PSMB capability). This would be a matter for each jurisdiction to decide on given its individual needs.

Common standards for interoperability should build on the *National Framework to Improve Government Radiocommunications Interoperability 2010–2020*, which was endorsed by all jurisdictions (through COAG) in 2009 to improve interoperability across LMR networks. The standards could also be informed by past work undertaken by the COAG Public Safety Mobile Broadband Steering Committee and COAG senior officials (chapter 1), as well as national technical standards that have been developed in the United States (FCC 2012) and other countries.

Police and emergency services ministers in each jurisdiction will need to lead efforts to agree on common technical standards, in consultation with their PSAs. There would be value in the Australian Government being included in this process, given its role in spectrum allocation and oversight of some PSAs.

Ideally, standards should be put in place within one year. This would allow time for standards to be developed while reducing the risk of 'early mover' jurisdictions locking in technologies that preclude future interoperability with other jurisdictions. Common standards should be updated on a periodic basis as circumstances or technologies change (for example, as new 3GPP standards incorporating public safety features are released).

Existing bodies can facilitate these inter-jurisdictional efforts. Several fora have already been established under the COAG Law, Crime and Community Safety Council, such as the National Coordinating Committee for Government Radiocommunications. Such bodies would also be well placed to publicly report on progress in PSMB implementation across Australia (on a regular basis) and to act as a forum for jurisdictions (and their PSAs) to formally share information and experiences relating to the procurement, adoption and use of a PSMB capability.

DRAFT RECOMMENDATION 7.2

To facilitate an interoperable mobile broadband capability for PSAs, state and territory governments should task police and emergency services ministers with agreeing to a set of minimum common technical standards within one year. These standards should have the objective of facilitating national interoperability and should build on the *National Framework to Improve Government Radiocommunications Interoperability 2010–2020*.

7.3 Spectrum allocation

The Australian Communications and Media Authority (ACMA), an independent Commonwealth agency, is responsible for regulating, licensing and pricing radiofrequency spectrum in Australia. In doing so, it is guided by the *Radiocommunications Act 1992* (Cwlth). It is also guided by directions from the Minister for Communications, for example, to allocate spectrum to particular uses or to price or sell spectrum in a particular way (Department of Communications 2015b).

Two main objectives set out in the Radiocommunications Act are to:

- maximise, by ensuring the efficient allocation and use of the spectrum, the overall public benefit derived from using the radiofrequency spectrum (s. 3(a))
- make adequate provision of the spectrum:
  - for use by agencies involved in the defence or national security of Australia, law enforcement or the provision of emergency services; and
  - for use by other public or community services (s. 3(b)).

ACMA has developed a set of supporting principles for managing spectrum. These include allocating spectrum to the highest value use, using the least restrictive approach to achieve policy objectives, promoting both certainty and flexibility, and balancing the cost of interference and benefits of greater spectrum utilisation (ACMA, sub. 14).

All mobile broadband networks require access to spectrum. In a commercial approach to delivering PSMB, services would be delivered over commercial networks using the spectrum holdings of their commercial operators (chapter 5). By contrast, a dedicated or hybrid approach would require access to spectrum in areas where a new network is established. Therefore, to pursue a dedicated or hybrid deployment approach, a state or territory government would need to obtain the right to access a suitable band of spectrum.

ACMA has set aside spectrum for potential public safety use

ACMA has recently made several decisions relating to public safety spectrum. Since 2010, it has been in the process of consolidating public safety (narrowband) communications into the Harmonised Government Spectrum portion of the 400 megahertz (MHz) band, in conjunction with the states and territories (ACMA, sub. 14). It has also been phasing in a model of opportunity-cost pricing for LMR apparatus licences in this band, in response to congestion in densely populated areas of Australia (ACMA 2015d).

In October 2012, ACMA made an in-principle decision to set aside 10 MHz of spectrum within the 803–960 MHz band (often referred to as the 800 MHz band) to support the deployment of a PSMB capability (ACMA, sub. 14). This would be in part of the band that aligns with 3GPP standards for LTE and is consistent with ongoing work through the International Telecommunication Union to identify parts of this band for public protection and disaster relief (appendix B). ACMA's decision was made as part of an earlier PSMB policy process that called for a single frequency band to be made available for PSMB (chapter 1). A final decision on allocation of this spectrum is yet to be made.

In 2013, ACMA allocated 50 MHz of spectrum in the 4.9 gigahertz band for exclusive use by PSAs (provided through a class licence). This frequency is suitable for several wireless technologies, including Wi-Fi, deployable LTE cells and air-to-ground communications.

Several inquiry participants, including state and territory governments, favoured a common band of spectrum being used by all states and territories to deliver a PSMB capability.

- Some argued that harmonisation with spectrum frequencies used elsewhere in the world can reduce equipment costs. In particular, the use of the same spectrum bands used in other countries — either for PSMB or commercial LTE — could allow PSAs to benefit from economies of scale in the design and manufacture of end-user devices (Alcatel-Lucent, sub. 15; BAI, sub. 1; Motorola, sub. 12; Rivada Networks, sub. 9; Telstra, sub. 19; Victoria Police, sub. 17), or potentially give them access to a greater range of equipment (Victorian Government, sub. 28).
- Participants also argued that use of a common spectrum band will be needed to achieve interoperability between PSAs in different jurisdictions of Australia (ATF, sub. 4; MFB, sub. 6; Motorola, sub. 12; NSW Telco Authority, sub. 30; Victoria Police, sub. 17; Victorian Government, sub. 28).

In addition, participants put forward views on the technical and cost considerations of different spectrum bands, and the need to allow PSAs to roam onto commercial mobile carrier networks. These matters are examined in chapter 5.

Any state or territory government that wishes to access spectrum for a dedicated or hybrid PSMB capability is not dependent on ACMA allocating spectrum for this purpose — it could apply to ACMA for an apparatus licence or obtain a spectrum licence, either at auction or from an existing licence holder (box 7.7). In doing so, jurisdictions would need to weigh up the costs and benefits of obtaining access to a particular band, based on the availability of particular bands and the bands used in other jurisdictions (including in jurisdictions that opt for a commercial approach to deliver PSMB using commercial spectrum).

Box 7.7 Spectrum licence types

The Australian Communications and Media Authority uses three main types of licence to allow access to spectrum.

- **Spectrum licences** grant exclusive use of a defined band of spectrum within a defined geographic area. These licences have the most protection from interference and can be used for any technology. Licences are issued for up to 15 years, with fees paid up front. They are typically sold at auction and can be traded on secondary markets. Examples include mobile phone networks and television broadcasting.
- **Apparatus licences** grant an exclusive right to use a specific transmitting device in a specific geographic location. Licences are usually issued for up to 5 years (and potentially longer for some devices), with fees payable annually. Licence holders can transfer the licence to another entity, or authorise third-party operation, provided the licence conditions continue to be met. Licences are generally renewed, unless there are policy or legal reasons to do otherwise. Examples include air traffic control systems, fixed wireless links and land mobile radio networks.
- **Class licences** permit shared public use of a defined band of spectrum for specific low-power or localised transmitting devices. There are no licence fees, since licences are not issued to individual users. Examples include wireless headsets, television remote controls and Wi-Fi.

In addition, transmitter devices must be separately registered and comply with regulations on transmission power levels and out-of-band emissions (to limit interference).

Sources: ACMA (sub. 14; 2013a, 2013c, 2015a); Department of Communications (2015b).

ACMA can make spectrum available for PSMB either by auctioning licences to the highest bidder, or by making an administrative allocation. Regardless of the approach used, any decision would need to be based on consideration of whether doing so would lead to the efficient use of spectrum. Central to this is weighing up the value in using spectrum to support public safety communications against alternative uses for the spectrum. In principle, using spectrum for public safety communications would only be efficient if the benefits of doing so (which may be non-monetary) exceed the opportunity costs — the value of the alternative uses (such as commercial mobile broadband).

ACMA (sub. 14) submitted that it would take into account the potential for a PSMB capability, along with the findings of this study, as part of its ongoing review of the 800 MHz band. This process will likely involve clearing currently used parts of the band to make spectrum available for mobile broadband or other uses, including in frequencies that are harmonised with 3GPP standards for LTE technology (ACMA 2012b; Motorola, sub. 12). Ultimately, ACMA will decide which specific frequencies and bandwidths to make available for sale or to allocate on an administrative basis.

This process is likely to present opportunities for jurisdictions that wish to pursue a dedicated or hybrid PSMB capability to purchase access to spectrum in the 800 MHz band (in line with bands set aside for public protection and disaster relief in the Asia-Pacific region (appendix B)). Allowing other users to bid for this spectrum would encourage its allocation to the highest valued use, and could potentially allow commercial mobile carriers to develop innovative solutions to meet PSA needs using the spectrum. In addition, jurisdictions would also be able to bid for any other spectrum (in other bands) that becomes available.

Ultimately, however, deciding how best to allocate and licence spectrum to meet the objectives set out in the Radiocommunications Act is a responsibility for ACMA. At this stage, the Commission does not consider that ministerial or other intervention in ACMA's processes for allocating spectrum for public safety would be warranted. However, the Commission notes the Australian Government's recent announcement that it will replace the current legislative arrangements for spectrum management with new legislation that streamlines licensing and improves flexibility (Turnbull and Fletcher 2015), in line with recommendations made by the Department of Communications (2015b) in its recent *Spectrum Review*.

Spectrum should be priced at opportunity cost

In the Commission's view, state and territory governments (acting on behalf of their PSAs) are best placed to assess the benefits of public safety spectrum, based on their individual needs, policy priorities and the costs of different PSMB delivery options. Where a jurisdiction has determined that a dedicated or hybrid PSMB capability is the best way forward, it would have a strong incentive to purchase access to spectrum where the public safety benefits exceed the costs.

In a competitive auction process, the cost of purchasing spectrum would reflect its opportunity cost — the value of the next best use. By contrast, if a decision is made to administratively allocate spectrum for a PSMB capability, ACMA should price it at its opportunity cost (plus any administrative costs involved in licensing). Either approach can facilitate the licensing of spectrum to its most efficient use from the perspective of the community as a whole.

The Commission has previously supported the use of opportunity-cost pricing for public interest uses of spectrum (PC 2002). This position has also been supported by ACMA (sub. 14) and the Department of Communications (2015b).

Opportunity-cost pricing can give states and their PSAs a strong incentive to use any spectrum they purchase in an efficient way. Where PSAs (or statewide implementation agencies) would require additional funding to cover the cost of spectrum, state or territory governments should provide this in a way that is not tied to the use of the spectrum (for example, through a general budget allocation) so as not to undermine incentives for PSAs to use spectrum efficiently.

DRAFT RECOMMENDATION 7.3

If the Australian Communications and Media Authority allocates spectrum for PSMB, it should be priced at its opportunity cost.

Licensing arrangements should be flexible

State and territory governments will need flexibility to purchase access to spectrum in a way that best meets their needs. Not all will require use of a large band of spectrum upfront, and some may benefit from having access to smaller or more localised bands, potentially over a short time period. For example, the Victorian Government (sub. 28, p. 6) advocated for an allocation of spectrum to the states and territories, and argued that ‘arrangements need to be flexible enough to accommodate differences between states and territories’.

ACMA has previously indicated, as part of the earlier PSMB policy process, that it would use an area-based apparatus licensing regime to authorise access to spectrum for PSMB (ACMA 2012a). Apparatus licences are already used for LMR and can be tailored to a specific geographic area or time period (box 7.7).

Ahead of a move to a single licensing system for spectrum (as recently announced by the Australian Government), apparatus licensing could provide jurisdictions with exclusive access to small and/or localised spectrum bands, potentially over a short time period. It could also allow jurisdictions to purchase licences upfront for later use. A flexible licensing approach would give each jurisdiction greater scope to trial a PSMB capability, such as by rolling out a dedicated network in particular areas. This would enable each jurisdiction to better evaluate the costs and benefits of a dedicated PSMB network, given its specific circumstances (section 7.6).

The opportunity costs of spectrum will vary depending on the nature of the licence and geographic location. This means that smaller, shorter or more geographically specific licences would likely be cheaper to purchase than a larger amount of spectrum allocated on a long-term or national basis (as was assumed for illustrative purposes in chapter 6).

Leasing can allow for more efficient use of spectrum

Even where a particular licence holder has exclusive access to some spectrum, there may be more valuable uses in particular times or places. By leasing or selling their access rights to a third party when they do not need spectrum (in exchange for payment), licensees can facilitate more efficient use of spectrum.

Most spectrum licence types allow some form of leasing — for example, apparatus licence holders can allow third parties to operate under their licence in certain situations, provided that the licence conditions are adhered to (and the other user has the technical ability to make use of the spectrum) (ACMA 2014f). However, public sector agencies (at the Australian Government level) have generally made little use of spectrum leasing where government budget policies have restricted them from retaining the proceeds of doing so (Department of Communications 2015b).

Several inquiry participants pointed to the potential benefits in allowing state or territory governments (or PSAs) to lease any spectrum they hold to other users when it is not required for public safety. This could occur by selling commercial mobile carriers access to the spectrum used by a dedicated PSMB network (or access to spare network capacity on a wholesale basis) during periods were public safety traffic is low. The large and infrequent nature of peaks in PSA traffic demand (chapter 4) mean that there is considerable potential for leasing spectrum when it is not utilised.

For example, the Police Federation of Australia (sub. 8) favoured the sharing of spectrum when not fully utilised by PSAs so that valuable spectrum is not wasted. VHA (sub. 11) and BAI (sub. 1) supported making spectrum available to other users when there is excess capacity on a PSMB network, while preserving priority access for first responders. Rivada Networks (sub. 9) put forward a model for doing this, whereby spare network capacity would be leased to mobile carriers (on a wholesale basis) to provide a revenue stream for PSAs, and 'ruthless pre-emption' technologies would allow PSAs to regain access to the full network capacity when required. The Victorian Government (sub. 28) argued that leasing arrangements could allow for greater economies of scale (where a larger network has lower unit costs to build) and allow more total capacity to be made available to PSAs during 'surge' events.

Spectrum leasing has been flagged as part of a PSMB capability in the United States (appendix B). It was also supported for public-sector spectrum holders more generally in the recent *Spectrum Review* (Department of Communications 2015b). In response to that review, the Australian Government announced that it would examine policy and financial arrangements for spectrum use by its agencies (Turnbull and Fletcher 2015).

The Commission supports spectrum leasing in principle as a way to make more efficient use of scarce spectrum. Where state or territory governments hold PSMB spectrum, they could sell access to other users during periods of excess capacity or on a temporary basis before a dedicated network is deployed (or, where spectrum is held by a state agency on behalf of the government, the government could change budget rules where these impede spectrum leasing). This would give jurisdictions greater flexibility in how to use spectrum as an input to a PSMB capability. However, spectrum sharing may only be practicable if PSAs can be assured that they will be able to access network capacity at times when they need it (chapter 5).

Current spectrum licensing frameworks can support spectrum leasing, and it will be important that conditions are not imposed on any PSMB licences that might inhibit this. Where individual jurisdictions purchase access to spectrum, they will need to weigh up the technical feasibility and risks associated with leasing it to other users against the benefits. In particular, contractual arrangements would need to clearly specify the conditions of any leasing and how public safety officers would be able to regain capacity in emergency situations.

7.4 The role of regulation

It would be unrealistic and uneconomic for a government to implement a PSMB capability without some form of private-sector involvement (section 7.5). However, commercial entities do not have the same incentives as governments — for example, commercial mobile carriers' shareholders generally expect them to maximise profits (PFA, sub. 8). As such, mobile carriers might not provide all the outcomes that PSAs want without some form of compensation or other government intervention.

Governments can attempt to secure outcomes that markets would not otherwise provide by using two types of tools: regulatory intervention and commercial contracts. In identifying the right tool to use, governments need to weigh up the costs and benefits to the community as a whole.

Study participants and earlier reports have identified several areas where regulation could help governments secure a PSMB capability.

Participants noted the potential for the National Broadband Network (NBN) to provide backhaul or satellite broadband services for PSMB (ATF, sub. 4; Coutts Communications, sub. 20; CSIRO, sub. 16; VHA, sub. 11; Victorian Government, sub. 28). Some suggested that this would need to be accompanied by regulatory intervention. For example, ARCIA (sub. 2) argued that the NBN could provide backhaul capacity with the facilities and prices under government control. The Centre for Disaster Management and Public Safety, APCO Australasia and Victorian Spatial Council (sub. 7) called for the operational premises of PSAs to be given high priority in the NBN roll out.

Other participants supported regulatory interventions relating to the delivery of PSMB services over commercial networks. For example, the NSW Telco Authority (sub. 30) argued for the regulation of prices and minimum service levels, and the Victorian Government (sub. 28) advocated for a regulatory framework at the Australian Government level to underpin priority access, quality of service and network management arrangements. These views echo the case put forward by an earlier parliamentary inquiry (PJCLE 2013). In addition, BAI (sub. 1) favoured mandating that all existing Australian mobile carriers allow public safety officers to roam onto their networks. VHA (sub. 11) raised the prospect of spectrum being sold to mobile carriers on the condition that PSAs are given priority access based on a set of pre-defined protocols.

Past studies have gone further, raising the possibility of using spectrum and carrier licence conditions to compel mobile carriers to provide a PSMB capability (either to be imposed from the outset, or in the case that commercial agreement cannot be reached). This could involve:

- placing conditions on new spectrum licences (ahead of auction) that require the licensee to provide a PSMB capability under specific price or non-price terms (Access Economics 2010), and potentially allow the spectrum to be reassigned to another entity if the services are not adequately provided (SCF Associates 2014)
- adding new conditions to the operating licences of mobile carriers to require them to provide PSMB services (Access Economics 2010; SCF Associates 2014) or allow PSAs to second commercial networks in defined emergency situations (PJCLE 2013).

Past inquiries have also raised the possibility of using legislative powers to compel mobile carriers to provide PSAs with access to spectrum or mobile networks during emergencies — for example, by enacting provisions in the Radiocommunications Act that could allow PSAs to access spectrum licenced to other users in a declared emergency (PJCLE 2013).

All the above forms of regulatory intervention would need to be implemented by the Australian Government (or its agencies), which has responsibility for regulating telecommunications services, infrastructure and spectrum. However, the case for these interventions is weak. Study participants did not put forward *specific* details of what regulatory interventions should be undertaken or why existing regulatory frameworks would not be appropriate.

Infrastructure access is already regulated

Existing regulatory arrangements in the telecommunications sector (box 7.8) are mainly designed to promote competition and the efficient use of, and investment in, infrastructure, especially in market segments and locations where there is only one supplier of a particular service. For example, the Australian Competition and Consumer Commission (ACCC) regulates access terms and prices for backhaul transmission (which is used to deliver mobile services) in some parts of Australia. The ACCC also administers a facilities access regime that provides an avenue for mobile carriers to access cell site infrastructure owned by other parties. This is supported by infrastructure-sharing provisions in industry codes.

Access regulations are implemented by the ACCC following careful and detailed analysis of a particular market. In deciding whether to regulate access conditions or prices, the ACCC carefully examines the impact that regulations may have on the efficient use of, or investment in, infrastructure (ACCC 2014b). Any additional regulations introduced for the purpose of a PSMB capability could potentially reduce incentives for future investment and ultimately leave the community worse off overall.

Competition laws apply to NBN infrastructure, just as they do to other forms of telecommunications infrastructure. While the NBN is owned by the Australian Government, it is operated on a commercial basis at arm's length from government. As such, any government intervention to compel access to NBN infrastructure would need to be based on evidence of a problem (such as market failure) and the ability for government intervention to remedy the problem without creating other problems.

In practice, access to NBN infrastructure would best be secured on a commercial basis. NBN Co is already trialling the connection of backhaul to mobile cell sites and expects to provide connections between cell sites and NBN Points of Interconnect in the second half of 2016 (NBN Co 2015a).

Regulation is a blunt way to encourage service delivery

Using regulation to compel private companies to deliver services to governments (or deliver services in a particular way) can be costly. Where regulations mean that a supplier is forced into providing a service, the supplier is likely to factor the cost of doing so into the prices it charges — or make calls for compensation. Regulations governing the telecommunications sector are already complex, and imposing further regulations could give rise to unintended consequences, such as reduced incentives for private-sector investment.

In addition, regulations on how a service is provided can limit the flexibility of suppliers to meet governments' objectives in the least cost way. In all cases, the ultimate cost to governments (and taxpayers) may not be transparent, making it hard to assess whether the benefits of the regulation outweigh the costs.

In particular, imposing conditions on spectrum or carrier licences that compel commercial mobile carriers to deliver services to PSAs could lead to sub-optimal outcomes. Spectrum licence conditions could only be imposed on *new* spectrum ahead of it being auctioned, and would complicate the auction process (Access Economics 2010). Such conditions could also lead to spectrum remaining unsold if bidders consider that it would no longer be worth purchasing at the reserve price — a situation encountered in the United States when the federal government attempted to auction spectrum with conditions requiring the licensee to deliver a PSMB capability (appendix B).

Box 7.8 Telecommunications regulation and policy

The Australian telecommunications sector is subject to various forms of regulation, some of which applies specifically to mobile networks.

The Australian Competition and Consumer Commission (ACCC) is responsible for the economic regulation of the telecommunications sector. It has powers to regulate service provision and set terms and conditions for third-party access to infrastructure.

Currently, the ACCC regulates mobile termination and backhaul transmission services (both of which are necessary inputs for the delivery of mobile services) under the *Competition and Consumer Act 2010* (Cwlth). Commercial backhaul services are regulated in many areas of the country, except where there is deemed to be sufficient competition (mainly between capital cities, within metropolitan areas and along some capital–regional routes) (ACCC 2014a). The ACCC does not regulate domestic mobile ‘roaming’ (where customers of one network can receive services from another network). However, commercial mobile carriers have voluntarily entered into roaming agreements at various times. At present, Vodafone has an agreement that allows its customers to roam on to the Optus network in some regional areas.

Under the *Telecommunications Act 1997* (Cwlth), the ACCC is responsible for administering provisions that deal with rights to third-party access to a defined set of facilities, including transmission towers, sites of towers (such as land and buildings) and underground facilities. These provisions are reflected in the Facilities Access Code, compliance with which is a carrier licence condition, although access arrangements are typically negotiated commercially before they reach arbitration by the ACCC (ACCC 2013).

In addition, the telecommunications industry has developed a guideline for how it will cooperate during emergency situations. This is designed to provide a standard procedure for carriers to cooperate with each other for emergency response. It specifies how carriers should work together when a pre-planned service provider cannot efficiently meet the requirements of the emergency services (Communications Alliance 2013).

Further, governments have subsidy schemes in place relating to the mobile sector. Some have initiated ‘black spots’ programs to subsidise the extension of mobile carrier networks in regional areas. For example:

- the Australian Government recently announced $100 million in funding for 499 new mobile base stations to be installed in regional areas by the end of 2018 as part of its Mobile Black Spot Program (Turnbull 2015). This is supplemented by funding from mobile carriers and state and territory governments. An additional $60 million of Australian Government funding has been allocated for a second round of the program. Winning bidders in the program are required to give other mobile carriers the opportunity to co-locate equipment on the new sites (including through sharing access to power and backhaul) (Department of Communications 2014a)
- in Western Australia, the state government contributed $39 million in 2012 to expand mobile coverage along highways and in remote towns as part of the state’s Regional Mobile Communications Project (WA Department of Commerce 2014). Telstra won the contract and has deployed 113 new base stations, which was expected to increase its coverage footprint in Western Australia by 31 per cent. While Telstra owns the infrastructure, it is required to allow PSAs in the state to co-locate their own radio communications equipment on each site.

Other policies are of more direct relevance to public safety, including Triple Zero and Emergency Alert. These are outlined in chapter 2.

Even if such spectrum were purchased, bidders would factor the cost of providing PSMB into their bids, meaning that the community effectively pays for PSMB services through lost spectrum revenues. Moreover, this model could lock governments in to using the mobile carrier that holds the spectrum licence for the duration of that licence (up to 15 years), or to any entity the carrier sells the licence to. Not only would this mean that the total cost of providing PSMB is not transparent, it may also be a more costly way to provide it than the alternatives.

Carrier licence conditions would give rise to a different set of problems. While conditions could be applied to existing carrier licences, governments would need to choose whether to impose the conditions on all mobile carriers (which could be surplus to requirements) or single out one or more specific carriers (which could affect competition in the broader market) (Access Economics 2010). Either approach may require legislative changes to be made and, since these would be retrospective, would inevitably lead to calls for compensation. Were this compensation not forthcoming, carriers could raise the prices they charge to all customers and/or reduce the service level provided to PSAs to the minimum permitted by the licence conditions. In addition, the imposition of licence conditions on all carriers (current and future) could raise barriers to entry in the mobile telecommunications market.

A further problem with regulatory compulsion is the difficulty of knowing in advance what specific services (or service quality) may be required in future. For example, even if PSAs' precise requirements could be detailed today, it may be difficult or impossible to adjust conditions imposed on spectrum licences in future as PSAs' needs change. This would mean that the conditions prove to be insufficient for future needs (Access Economics 2010), or limit PSAs' flexibility to adjust a PSMB capability to meet their evolving requirements.

Contracts offer an alternative to regulation

Voluntary contracts offer a flexible alternative to many forms of regulation, and are the norm in most areas of government infrastructure and service delivery involving private-sector participation. While reaching agreement on terms and prices that are acceptable to both parties can be challenging, contracting offers considerably more flexibility to identify innovative and low-cost solutions, and to adjust arrangements over time as requirements change. Regulatory compulsion should only be used as a matter of last resort if commercial negotiations fail, and following a thorough evaluation of the costs and benefits (including an assessment of the least costly form of regulatory intervention).

Commercial negotiations can be difficult in markets where there is a small number of suitable suppliers, or where a single supplier wields considerable market power. But ad hoc regulations requiring certain services be provided to governments are an indirect and likely ineffective way to address these market imperfections. As noted above, regulatory frameworks are already in place to address a lack of effective competition in telecommunications markets. Moreover, governments have a range of options for counterbalancing the bargaining power of a commercial service provider that they can exercise through procurement and contracting (section 7.5).

7.5 Public procurement

The private sector will play an important role in the implementation of a PSMB capability. This could include some combination of (but would not necessarily be limited to):

- designing, planning and constructing a mobile broadband network
- providing broadband services over a commercial mobile network
- providing operational and maintenance services
- providing equipment (such as end-user devices) or other inputs (such as backhaul)
- making space on mobile cell site towers available for PSMB equipment
- delivering user training
- developing software and end-user applications.

The exact role will likely depend on the PSMB deployment approach taken in each jurisdiction and the costs and benefits of using the private sector (relative to governments delivering these services themselves). For example, even in the case of a dedicated network, governments will need to rely on commercial entities to supply and/or install equipment.

Private-sector involvement can allow governments to draw on the expertise and experience that commercial mobile carriers and technology companies have with the development, use and deployment of mobile broadband technologies. For example, commercial entities tend to be more adept than governments in adopting new technologies and innovating to meet consumers' needs at least cost (Telstra, sub. 19). The private sector has also tended to bring more rigour to the assessment of the costs and risks of infrastructure projects than governments have (PC 2014b).

However, good procurement is difficult. Governments do not have perfect information about companies' cost structures, technical capabilities or intentions. This means that procurement processes need to be carefully designed to elicit the least-cost provider of a service, leverage competition, allocate risks and agree on prices. There are several leading practices that can guide governments in this process, as set out in the Commission's recent inquiry into public infrastructure (PC 2014b). Some of these are elaborated on in greater detail throughout this section.

Value for money should be the primary consideration

In most government procurement, achieving value for money is the primary objective. This generally means obtaining a fit-for-purpose outcome from the private sector at least cost. In the case of PSMB, this would mean meeting all the elements that define a 'public safety grade' service (chapter 4).

Some study participants raised additional objectives that could be targeted through PSMB procurement. For example, procurement could be designed to:

- avoid adverse impacts on competition in the broader mobile communications market (VHA, sub. 11)
- promote competition in specific market segments (such as in regional Australia) (Rivada Networks, sub. 9)
- meet other potential policy objectives, such as promoting universal access to mobile communications in regional areas (Optus, sub. 18).

There may well be opportunities to target such objectives through the delivery of new infrastructure or pro-competitive conditions placed on PSMB contracts. However, in the Commission's view, PSMB procurement would be a blunt tool for targeting these other policy objectives compared to the alternatives. In particular, legislation governing competition and infrastructure access in telecommunications markets is already in place and administered by the ACCC, and a range of separate government programs are already used to improve services in regional Australia (such as black spots programs) (section 7.4).

Attempting to target additional objectives through PSMB procurement may not necessarily be a lower cost or more effective way of meeting these objectives, and would make the total cost to taxpayers of implementing PSMB (separate from achieving other policy objectives) less transparent. Targeting additional objectives could also introduce complications and delays to the tendering process, for example, due to additional complexity or impacts on private sector participation.

In tendering for parts (or all) of a PSMB capability, state governments (or PSAs) should seek to obtain value for money — that is, the best possible outcomes for the community as a whole, taking account of quality and risk as well as cost. This would mean identifying the least-cost way to meet the service requirements of PSAs while complying with common national standards to support interoperability across jurisdictions.

Where governments wish to target other policy objectives, there should be a robust and transparent analysis of all available policy instruments. Other objectives should only be targeted through PSMB procurement where that is the least-cost way of doing so, and where any impact on the cost of procurement is explicitly identified and made public. Where governments are concerned about the impacts that procurement processes may have on market competition, they should first consider the adequacy of available ways to address any adverse impacts on competition (such as existing legislation administered by the ACCC) before altering procurement practices.

DRAFT FINDING 7.2

Using procurement processes for PSMB to target policy objectives other than value for money — such as promoting competition in parts of the broader mobile broadband market or meeting equity objectives — would be a blunt, costly and non-transparent way to meet those objectives. Other policy instruments are likely to provide more effective alternatives for achieving additional objectives.

Competitive tendering can reduce costs and improve outcomes

Tendering is a standard and well-established feature of government procurement. It allows governments to seek proposals from a range of private-sector parties (including individual companies and consortia of companies) and select the proposal that meets their requirements at least cost. This process can encourage companies to bid competitively to win the tender.

Yet tenders are complex to design, and the tender process can have a direct bearing on the final delivery cost of projects (PC 2014b). For example, highly specific design requirements can reduce the risk that policy objectives are not met and make it easier for governments to compare submitted bids. But too much specificity can limit bidders' flexibility to innovate and put forward lower-cost solutions. It can also deter some bidders if bids become too costly to develop, or if the project becomes too large or complex for some companies to handle — and thereby reduces competition (PC 2014b).

There are challenges specific to the Australian telecommunications sector

The challenges of designing a good tender process — and benefiting from competition between bidders — are amplified by features of the mobile telecommunications market in Australia (box 7.9). There are three commercial mobile carriers, which compete on coverage, price and service offerings. While all offer a high level of population coverage (above 95 per cent), there is wide variation in their geographic footprints.

In some parts of the country (especially regional Australia), only one commercial network is available, or there is only a single provider of backhaul transmission. While a single network can sometimes be economically efficient — where it can meet customer demand at lower cost than multiple networks — it can mean there is less consumer choice in particular areas. Moreover, the extensive physical infrastructure (such as base stations and radio networks) required to provide mobile broadband coverage means that expanding a network is expensive. As a result, potential competitors can face high barriers to market entry given that an operator would need to make significant capital expenditure to effectively compete (Optus, sub. 18).

Markets for network equipment and end-user devices may be more competitive, since these markets are effectively global. However, Australia is a small part of the international market and may effectively be a 'price taker', with limited influence over what equipment is manufactured. Moreover, there are relatively few major suppliers and most have ongoing commercial relationships with the Australian carriers.

Box 7.9 Mobile telecommunications markets in Australia

Since the early 1990s, several companies have constructed mobile phone networks in Australia. The specific technologies have varied over time, starting with analogue services, 2G digital, 3G and 4G. Each technology has generally required a significant upgrade to infrastructure and equipment, and has co-existed with earlier technologies. Many handsets can operate across different types of network.

There are three mobile carriers at present: Telstra, Optus and Vodafone Hutchison Australia (other carriers have had a market presence in the past). Telstra has the largest 3G network, covering around 2.3 million square kilometres and 99.3 per cent of the population, followed by Optus (around 1 million km^2 and 98.5 per cent of the population) and Vodafone (350 000 km^2 and 95.4 per cent of the population). In addition, a number of other companies (known as Mobile Virtual Network Operators) lease wholesale capacity from mobile carriers and sell services to retail consumers.

A separate market exists for backhaul transmission (the links, usually fibre-optic cable, between mobile base stations and the rest of the network). While there are many providers nationally, in many regional areas Telstra is the only provider.

Competition in the retail market is generally strong (especially for data services), and overall costs to consumers have been falling in recent years. For example, in June 2014, Telstra had a 45 per cent share of the retail market for mobile handset services, Optus 27 per cent and Vodafone 18 per cent (virtual operators comprised the remainder).

However, competition in the wholesale market is limited by the nature of mobile network infrastructure — in some areas, customer demand might only support the presence of a single network. Nevertheless, there is significant infrastructure-based competition, with consumer demand strong enough to support the presence of multiple networks in many metropolitan and regional areas.

Sources: ACCC (2014a, 2015b); Analysys Mason (2015); Optus (sub. 18); Telstra (sub. 19).

Study participants drew attention to the limits of competition in the mobile telecommunications market. For example, VHA (sub. 11) noted that Telstra's large holdings of spectrum and backhaul infrastructure in regional areas make it difficult for other mobile carriers to enter and compete in these areas. The Victorian Government (sub. 28, p. 8) argued that 'the degree of competition and the level of coverage provided by commercial networks is less than that required to provide PSAs certainty of accessibility, affordability and quality of service'.

A small number of potential commercial partners for governments to contract with, coupled with high barriers to market entry, can raise the risk that tender processes will not be competitive. Governments could be left with few choices of supplier and 'monopoly price' bids that significantly exceed the underlying costs of supply. For example, if there was only one company that a government could contract with to deliver a PSMB capability, that company may have an incentive to inflate its bid (up to the expected cost of the government delivering the solution itself).

A small number of potential commercial partners also introduces other risks into the procurement process. One is that the tender attracts no bidders. A supplier might consider that the benefits of the contract (additional business) do not sufficiently compensate for the costs and risks (such as the impacts on its other customers, costs of specific design requirements, reputational risks of failing to meet the government's needs, or the potential impact on its ability to compete in other markets).

There is also a risk that the commercial partner breaches the contract (or chooses to pay penalties specified in the contract rather than undertake specific actions). It may have an incentive to do so if it faces little effective competition, or is able to hold the government 'hostage' by revising prices after a large initial investment has been sunk.

However, governments are not powerless in dealing with mobile carriers and technology providers. They have several tools at their disposal to strengthen their bargaining position and/or facilitate competition in tender processes to deliver better value for money for taxpayers. These can be used to secure more competitive outcomes regardless of how frequently contracts are retendered.

Benchmarking and transparency can shine a light on cost structures

Information can help governments to assess bids that are submitted through a tender process. Once a jurisdiction has decided on the specific nature of the PSMB capability it wants to implement (including capacity, service quality and coverage), it could 'benchmark' cost information in the bids submitted. This would essentially mean identifying comparable cost estimates from available sources (including internationally) to gauge whether the costs put forward in a bid are broadly reasonable and/or where further explanation needs to be sought from a bidder.

In addition, transparency can be valuable after a contract is signed. Many government contracts for infrastructure construction and delivery include 'open book accounting' provisions, where the government client is able to inspect the supplier's financial records to assess the realised costs of construction (PC 2014b). Some have suggested that similar provisions be included in contracts for the delivery of PSMB services (TCCA 2013b), although governments would need to consider to what extent this might deter companies from bidding in a tender process.

Splitting up tenders can encourage greater competition

A more substantive strategy to improve competition in tender processes is to split a large project into a package of components, each of which is tendered separately (where this does not substantially undermine the efficiency of procurement or project delivery) (PC 2014b). This is likely to improve contestability and competition since the number of suitable suppliers tends to diminish as project size increases — for example, there would be very few companies that would be able to provide PSMB across the whole of Australia.

Splitting up tenders can also help where particular project elements require specific expertise, or timeframes mean that some elements need to be completed before others. Further, it can help to spread risk (and complexity) among a greater number of entities, thereby making it more attractive for a wide range of companies to participate and potentially leading to better overall risk management (NSW Legislative Council 2012; PC 2014b). Procurement guidelines issued by some state governments already support such an approach where it can improve value for money (for example, VDTF 2013).

The delivery of PSMB could be broken down into a package of tenders in two main ways:

- by technology or service — for example, tendering separately for infrastructure construction, service delivery over commercial networks, maintenance, end-user devices and training
- by geographic region — tendering separately for defined regions, for example, based on population density (metropolitan, suburban, rural) or the coverage footprints of existing mobile carriers (areas with multiple carriers separate to areas where only one carrier has coverage).

Such approaches have been used in procurement in other countries and sectors, including for PSMB (box 7.10). In addition, the Victorian Government (sub. 28, p. 9) submitted that 'Victoria considers it essential to unbundle procurement of network, services and terminals and avoid proprietary solutions'.

A further approach is to sign contracts with multiple mobile carriers in the delivery of a commercial or hybrid PSMB capability. For example, this might be done by signing a contract with one carrier to deliver a main service (with some network hardening) and a separate contract with another carrier to provide 'overflow' capability when additional capacity is required. Roaming agreements with multiple networks could also offer a way to provide greater reliability and redundancy for a PSMB capability (chapter 5). Some study participants expressed support for a multiple-carrier solution (for example, Coutts Communications, sub. 20; CSIRO, sub. 16), although there were diverging views among carriers (box 7.11).

At this stage, the Commission sees merit in state governments (or their PSAs) tendering by technology or service, similar to how tendering occurs for some other government projects. It also sees particular value in tendering for the delivery of PSMB services or infrastructure by geographic region (under any deployment approach). This would involve entering contracts with multiple carriers where doing so offers the best value for money, following an open and competitive tender process.

However, a disaggregated tendering approach would pose costs and challenges that governments would need to work through. First, there would be administrative or transaction costs associated with preparing multiple tenders and evaluating a higher number of bids.

Box 7.10 Public procurement in other sectors and countries

Various techniques have been used to improve competition in public procurement processes by breaking large projects into smaller parts, or by engaging multiple suppliers, both in Australia and in other countries.

Rail projects in New South Wales and Victoria

Breaking large projects into packages of smaller contracts has been used to increase competitive tension in rail infrastructure procurement in some states. For example, the NSW Government used packages of contracts (covering tunnel and station works, surface and viaduct works, and operations and maintenance) for its North West Rail Link project (Transport for NSW 2012), and has taken a similar approach to other large urban rail projects (NSW Legislative Council 2012). The Victorian Government used a package of six contracts, split up geographically, in the delivery of its Regional Rail Link project (VDTF 2013).

Australian Government air travel services

The Australian Government procures some air travel services on a 'whole of government' basis. In doing so, it has established a panel of airlines to provide both domestic and international services to government employees (Department of Finance 2015). Agencies are required to use the 'lowest practical fare' over four airlines when booking domestic flights.

PSMB in the United Kingdom and United States

Other countries have sought to improve competition in PSMB procurement by splitting tenders into a package of smaller contracts. In the United Kingdom, tendering for a national Emergency Services Network was split into four 'lots', each covering a different aspect of service delivery. Requirements were imposed for the suppliers of mobile network services and end-user services to be independent (although a single entity could submit bids for both), and for the provider of overall program management to be independent of the suppliers of other components (UK Home Office 2014).

In the United States, FirstNet has proposed breaking up procurement of a national PSMB network on a regional basis to increase competition among potential suppliers. Suppliers would be able to bid for one or more regions, or on a nationwide basis (Moore 2015).

Second, there would be costs in achieving coordination across multiple infrastructure or service providers. For example, if different mobile carriers were to win contracts in different regions, roaming arrangements would need to be put in place to allow PSAs to move between networks. This would give rise to technological and pricing complexities that need to be resolved (chapter 5), as well as complexities for governments in managing the tender process. Insistence on common technical standards and roaming agreements as part of the tender process could help to address these challenges.

Box 7.11 Views on a multiple-carrier solution

Optus (sub. 18) submitted that allowing PSAs to access more than one mobile carrier network could lead to greater reliability. This is because the use of more disparate and geographically dispersed infrastructure could reduce the risk of a 'single point of failure' (for example, due to power outages or extreme weather events) causing one network to go down.

VHA (sub. 11) also favoured a model where PSAs can access multiple networks, which could lead to greater network capacity being available during critical incidents, maximise the use of spectrum and create greater redundancy in coverage. VHA further submitted that this could maximise contestability in procurement.

Telstra (sub. 19) had a different view. It submitted that a national partnership with a single commercial network operator would be the only realistic way to provide PSMB, given the need to provide rural coverage and the potential for fragmented implementation and coverage across states under a more disaggregated model. Telstra also drew attention to some of the technical challenges posed by roaming across networks.

Third, in some cases, a single bidder might be able to deliver services across multiple regions, or deliver related services, at a lower total cost than a mix of separate bidders (due to economies of scale or scope). In these situations, awarding contracts for separate regions or services to separate companies could be inefficient.

In determining the size and scope of contracts, governments will need to weigh these costs against the potential benefits that could be obtained from a more competitive procurement process (IC 1996). In some cases, it may be possible to improve contestability without necessarily incurring high coordination costs or forgoing economies of scale. For example, allowing joint bids from consortia of suppliers (or allowing some tasks to subcontracted out) can allow for competition where there are few individual suppliers that could credibly provide the service at a large scale (IC 1996), or where it would be more costly for governments to take on the task of coordinating the activities of separate suppliers.

Allowing suppliers to choose whether to bid for a single geographic region or multiple regions can also create competitive tension. Even where a single company could supply all regions at lowest cost, the presence of competition in individual regions would put competitive discipline on the bids submitted. This kind of approach has been proposed as part of procurement for a PSMB capability in the United States (box 7.10). It would be preferable to restricting the number of regions a single supplier can bid for, as that may effectively forgo any economies of scale that result from using a single provider.

However, in some regions there may only be a single bidder — with a potentially inflated (above-cost) bid — or no bidder at all. This problem is likely to arise in any tendering process where a single supplier is dominant in parts of the market. While splitting tenders up geographically cannot avoid this problem, it does allow regions with limited competition (such as rural and remote areas) to be treated separately from regions where competition is greater. Where there is a risk that a supplier that is dominant in one region might use this dominance to 'cross subsidise' its bids in other areas (thereby allowing it to artificially reduce its bid price for those areas below that of its competitors), governments could consider requiring suppliers to bid for regions with limited competition separately. This separation of contestable from non-contestable elements would allow for greater transparency in bids and is generally considered part of good-practice procurement (IC 1996).

Negotiating collectively can exert countervailing power

Where potential suppliers possess market power, governments can exercise countervailing power by acting as a single entity in procurement. In the case of PSMB, this would occur where a statewide agency is tasked with procuring a single jurisdiction-wide capability (section 7.1).

Having a single government body across the negotiating table (as opposed to dealing with multiple PSAs separately) would mean that private-sector bidders have to deliver on the project requirements at a reasonable cost or risk not getting the business. In principle, governments could add further discipline by using the threat of withdrawing future government work. This centralised approach might also ward off a situation where a large commercial partner attempts to play off multiple government agencies against each other. It would also offer benefits in terms of economies of scale in equipment purchasing and reduced scope for duplication across PSAs (section 7.1).

However, there are limits to what centralised procurement can achieve. The size of a PSMB contract is likely to be small relative to a commercial mobile carrier's total revenues, meaning that the loss of business may not be seen as a significant business risk (although this may depend on the jurisdiction and could be influenced by competitive dynamics in the market). And, as discussed below, centralised procurement may achieve little if governments do not have a credible outside option.

Infrastructure and spectrum holdings can give governments leverage

State and territory governments (and PSAs) already own substantial assets that could be used as inputs to a PSMB capability. This includes a large number of LMR sites and associated infrastructure (such as towers, power supplies and backhaul), in addition to apparatus licences to use spectrum, mostly in the 400 MHz band. Jurisdictions may also have further spectrum at their disposal if they choose to purchase it for a PSMB capability.

Jurisdictions' bargaining power in commercial negotiations will depend, to a large degree, on the extent of their outside options. Ownership of infrastructure and spectrum gives a jurisdiction an option to bypass a potential supplier and build a dedicated PSMB capability itself (for example, in a specific area, while retaining the option to use mobile carriers to expand the network further). This can give it additional leverage in negotiations. It could also potentially reduce the cost of a contract, for example, where use of existing government assets reduces the need for new investment or where the ability to share spectrum with a supplier (section 7.3) induces lower bids (that take into account the value of this spectrum sharing).

However, the additional bargaining power could be limited by several factors. Foremost, it would depend on whether a jurisdiction is able to purchase access to spectrum in a nationally harmonised band for PSMB (section 7.3). Bargaining power could be constrained where jurisdictions choose to maintain a separate LMR capability in some areas, limiting the amount of infrastructure and/or spectrum that can be used for PSMB. And, not least, building a dedicated PSMB capability without mobile carrier involvement would only be a credible threat if governments can do it at reasonable cost.

Jurisdictions therefore will need to carefully consider how best to leverage their existing infrastructure and spectrum holdings during commercial negotiations, and in deciding whether to purchase access to additional spectrum.

Open standards and short contracts can reduce the risk of 'lock in'

A challenge in any public procurement process is minimising the risk of being 'locked in' to a particular supplier. This can occur where a contract involves delivering infrastructure or equipment that is highly customised and which another supplier is unable to supply (for example, because it is proprietary technology protected by intellectual property law, or because other suppliers are unable to replicate it at reasonable cost). Once this technology has been put in place (and the investment is 'sunk'), the supplier may have scope to behave opportunistically, such as by raising prices or refusing to supply newer technologies. Governments may face high costs or other impediments (such as legal action) in attempting to switch to an alternative provider.

Being locked in to a single supplier could also give that supplier an advantage over its competitors in future contract negotiations, to the extent that the initial investments reduce its costs of supplying the service in the future. This would reduce the ability for governments to secure competitive tendering outcomes over time (that is, in future procurement).

The risks of being locked in to a non-standardised solution offered by a single supplier were emphasised by many study participants (ACMA, sub. 14; Alcatel-Lucent, sub. 15; CDMPS et al., sub. 7; Coutts Communications, sub. 20; NSW Telco Authority, sub. 30; Telstra, sub. 19; VHA, sub. 11; Victorian Government, sub. 28). While this risk can arise under any PSMB delivery option (chapter 6), there are ways to reduce it.

Lock-in problems can sometimes be avoided through the careful crafting of contract clauses. But not all future contingencies can be foreseen at the time of contract negotiation, or even reflected in contracts. For example, if a new and unexpected mobile broadband technology or application were to emerge and PSAs wished to use it as part of a PSMB capability, they might only be able to do this on the prices and terms set by the company that provides the capability. Moreover, being locked in to using one particular supplier's technology could reduce a government's ability to switch to a lower-cost supplier in future (or raise the cost of switching). There is also a risk that the proprietary technology becomes outdated over time because it is incompatible with newer technologies or the supplier discontinues it.

Several strategies are available to governments to reduce the risk of being locked in to a single supplier. One is to use short contracts to allow for more frequent renegotiation or tendering, and thereby improve contestability. This can allow for more competition in the tender process and give governments more flexibility to respond to unanticipated contingencies (IC 1996) — such as some of the complexities that might arise once mission critical voice services can be delivered over LTE networks (chapter 5). Some participants explicitly favoured avoiding long-term contracts in the delivery of PSMB (for example, NSW Telco Authority, sub. 30).

However, tendering is a costly process, and the administrative and transaction costs can quickly add up when it is done repeatedly. Shorter contracts would also mean that the cost of capital investments made by the commercial partner would need to be amortised over a shorter period — thus raising the amount that governments would need to pay each year. This could increase the risk for the commercial partner (inducing them to submit higher bids, or no bid at all) and raise the risk that investments are written off before the end of their economic life (which may not be efficient).

Where large capital investments are required, a different strategy may be needed. In constructing a dedicated PSMB network, governments could use franchise contracts whereby the network is constructed and managed by a commercial partner but the assets (including spectrum) remain under government ownership. This would increase governments' ability to switch to an alternative company in the future (NSW Telco Authority, sub. 30). Where solutions involving mobile carrier networks are pursued (and require hardening or other investments in those networks), governments can align the length of contracts with the economic life of assets as a way to avoid being locked in to a provider for longer than necessary. Using multiple service providers to provide services and/or equipment can also reduce potential for lock in (NSW Telco Authority, sub. 30).

Under any deployment approach, insisting on the use of technology that complies with open international standards can improve governments' ability to switch suppliers in future. Although such requirements would be unlikely to increase the number of potential bidders for an initial contract, they can help to achieve procurement that is more competitive over the long term. A more general principle is to keep any customisation of infrastructure or equipment to a minimum, for example, by using existing infrastructure as far as possible.

Common national standards may assist in this process (section 7.2). Once these standards are set, they would send a strong signal to potential suppliers about the minimum requirements that would need to be met through PSMB to provide the technical interoperability that jurisdictions require (including the ability to roam onto other networks).

DRAFT RECOMMENDATION 7.4

If state and territory governments decide to deploy a PSMB capability, they should maximise value for money in procurement by using competitive procurement processes. In doing so, they should adopt strategies to increase the number of potential bidders (such that all Australian commercial mobile carriers would be able to participate) and reduce the risk of becoming 'locked in' to a single supplier.

Strategies available to governments include:

- benchmarking bids against other cost data and making tender processes transparent
- splitting up tenders by service and/or region
- negotiating on behalf of their PSAs
- leveraging their infrastructure and spectrum holdings in negotiations
- using short-term contracts that require adherence to national technical standards and the ability of public safety officers to roam onto other networks.

Efficient risk allocation can minimise costs

All contracts allocate risk. This can be done explicitly or implicitly. In some cases, the true 'owner' of a risk may not be known until something goes wrong (or the contract is disputed in the courts).

In allocating risks, governments need to consider who can manage those risks at least cost. Good practice is usually to allocate a risk to the party that is better placed to reduce the underlying risk, or can do so at lower cost. Where this is not feasible — or neither party can reduce the risk better than the other — the risk should be allocated to the party that is better able to absorb the risk (either by purchasing insurance or by bearing the consequences when the risk is realised) (PC 2014a, 2014b).

Where governments allocate a risk to a commercial partner, this will be factored into the price that suppliers are willing to bid for a contract (even where markets are fully competitive). This can be an efficient outcome. Where governments instead retain a risk themselves, there will also be a cost — in terms of mitigating that risk or bearing the consequences if it is realised. Ultimately, governments will face some kind of cost associated with all risks a project is exposed to.

The question then is who each risk should be allocated to. Efficient risk allocation — allocating risks to the party that can manage them at least cost — can minimise the long-term costs of delivering a project. Doing this transparently (including by sharing information on risks as part of the tender process) can also make it easier for each party to assess their risk exposure and facilitate greater interest in bidding for a tender (PC 2014b).

However, in making decisions about risk allocation, governments need to think through the impacts on private parties' willingness to bid for or enter into a contract. They will also need to take into account risks that cannot easily or credibly be transferred to a commercial partner, and so must inevitably be borne by governments. This includes the risk that service delivery breaks down and services are not provided to the community — as has happened prominently in Australia in some transport infrastructure contracts (PC 2014b).

Commercial partners are better placed to manage supply-side risks

The commercial partner in a PSMB contract would be better placed than governments or PSAs to reduce some risks, or to bear those risks if they are realised. These include risks associated with supplying products or services. For example, a commercial mobile carrier would generally be better placed to manage risks to equipment costs, construction times or technology changes. While the carrier may not be able to reduce other risks (such as earthquake risk), neither may governments, and allocating these risks to the carrier could strengthen its incentives to minimise the consequences of these events on PSA communications (provided that standard 'force majeure' provisions do not apply in such contracts (Access Economics 2010; TCCA 2013b)).

Governments can allocate supply-side risks to a commercial partner by expressing project requirements in terms of outcomes rather than inputs. By specifying the outcomes that governments are seeking (such as quality of service over a mobile network), a tender or contract can strengthen the commercial partner's incentive to meet these outcomes at least cost (since payment depends on achieving these outcomes). This would also give the supplier flexibility to change its mix of inputs in response to unexpected changes in costs, demand or technology (Competition Policy Review 2015; IC 1996).

For example, a mobile carrier delivering PSMB over its own network (a commercial approach) could achieve an agreed network reliability level through installing power supply backup at all its base station sites, hardening these sites, or increasing redundancy in cell overlaps and backhaul connections (chapter 5). Or the carrier could meet a given capacity requirement by installing more base stations, changing how it uses the spectrum it holds, or deploying transportable cells for large planned events. The best mix of these inputs will depend on many specific factors that the carrier is better placed to understand (and adapt to) than governments — such as the location of each site, relative costs and the network resources used to meet the demand from other customers.

Further, specifying contracts in terms of outcomes can give the commercial partner an incentive to manage supply-side risks that are not easily identifiable at the time a contract is signed, or that are not well understood by governments. Making contracts 'technology neutral' can help governments avoid being overtaken by rapid advances in technology, especially when procurement is protracted or long-term contracts are signed (CDMPS et al., sub. 7). Together with requiring adherence to open international standards, outcomes-focused and technology-neutral contracts can help governments to avoid project delays and/or being locked in to a high-cost solution.

Governments are better placed to manage demand-side risks

Some risks are better borne by governments or PSAs. These include the risk that PSAs' capacity requirements end up higher or lower than was originally envisioned when a contract was signed, or that quality of service needs change. These contingencies will need to be accounted for in contracts, as failing to do so would limit the ability to alter the PSMB capability if PSAs' needs change.

Typically, this is done through pricing arrangements — clauses that specify who will bear the cost of changing the capacity or quality of service. Making governments bear this cost (on behalf of their PSAs) would encourage them to trade off the value of service alterations against the cost. By contrast, if the commercial partner had to bear the cost, it would factor this risk into the amount it bids for the initial contract (or might even withdraw from bidding if its exposure to future costs is highly uncertain).

Governments and PSAs are better at managing these demand-side risks. They have the flexibility to decide if and when they need to expand a PSMB capability. By bearing the cost of doing so, they are encouraged to manage their demands on the network in other ways, based on an assessment of relative costs and benefits. For example, where PSAs have to pay for capacity expansions, they have an incentive to delay some non-urgent traffic or prioritise certain users or applications over others (section 7.1).

7.6 A phased approach to implementation

Flexibility will be of considerable value, regardless of when or how each state or territory government chooses to implement a PSMB capability. Remaining flexible to unexpected developments (such as in technology, demand or market structure) can be of considerable value in the face of uncertainty (chapter 5). It can also help governments and PSAs to implement a PSMB capability that meets their needs at least cost. The timing of PSMB investment offers opportunities for flexibility. While the commission used a range of capability levels in its illustrative evaluation of PSMB delivery options (chapter 4), none of these are necessarily the best *starting point* for any jurisdiction. More work needs to be done to better assess the costs, benefits and risks of available delivery options in each state and territory.

Trials would have considerable value

There would be merit in jurisdictions starting with a series of trials of PSMB. This might involve, for example, small-scale trials on short-term contracts, such as in inner-city areas (where the net benefits of PSMB are likely to be greatest). This approach was explicitly supported by some study participants (for example, Victorian Government, sub. 28). Moreover, the NSW Telco Authority (sub. 30) submitted that it will undertake a PSMB trial in September 2015.

Trials would have considerable value, including the ability to test the market, better understand and benchmark costs, and to systematically evaluate how PSAs use the PSMB capability and the benefits this generates. In particular, trials would allow for more thorough investigation of the risks associated with commercial deployment approaches — which offer the most cost-effective way to deliver PSMB — and ways to mitigate these risks (chapter 6). Only in the event that these attempts fail would it be appropriate to consider the merits of using dedicated spectrum to deliver PSMB services. Investing in dedicated spectrum *in anticipation* of commercial mobile carriers failing to deliver the requisite services would represent a highly risk-averse and costly strategy.

In the Commission's view, there is likely to be sufficient time for robust trials to be run and evaluated by jurisdictions ahead of 2020. Drawing on the lessons gleaned from trials, jurisdictions could then expand a PSMB capability (or deploy a higher-grade capability), subject to a suitable business case.

Using a phased approach to do this would offer further benefits, and was supported by several participants (for example, ATF, sub. 4; Ericsson, sub. 10). Phasing can help jurisdictions avoid making large and irreversible investments before they need to. It can also make it easier to benefit from lower-cost technology solutions as they emerge. This is because phasing allows scope to collect information and resolve uncertainties over time.

Some uncertainties are beyond governments' control, such as when (or whether) mission-critical voice communications can be delivered over LTE technology (chapter 5). Other uncertainties can be influenced by governments — such as the time it would take to undertake procurement and finalise contracts, or to roll out a new mobile network — but only to a limited extent. In any case, LMR voice networks will continue to be available for at least the next 5–10 years in all jurisdictions (chapter 5), creating a relatively low-risk environment for experimentation with a new technology.

DRAFT RECOMMENDATION 7.5

If state and territory governments decide to deploy a PSMB capability, they should take a phased approach to implementation by first trialling a capability on a small scale. Trials would provide an opportunity to:

- demonstrate the technical feasibility of a commercial approach
- evaluate the costs, benefits and risks of PSMB
- develop protocols and procedures for information and capacity sharing by PSAs
- develop the business case for a wider-scale rollout.

Land mobile radio networks are expected to continue operating in all jurisdictions for at least five years, creating a relatively low-risk environment for experimentation with PSMB.

Each jurisdiction has different needs

The best way to time investments in PSMB will depend on each state or territory's circumstances, such as its population distribution, geographic area, natural hazard profile, existing infrastructure and the coverage footprints of mobile carrier networks (Victorian Government, sub. 28). It will also depend on whether a jurisdiction wishes to pursue a PSMB capability, and on other government priorities and constraints.

There may be scope to reduce the costs of implementing PSMB by coordinating it with other investments. These could include state or Australian Government initiatives to invest in telecommunications in regional areas (Victorian Government, sub. 28).

LMR investments would also need to be taken into account. Some jurisdictions have LMR networks that are nearing time for replacement, while others have recently made new investments in LMR (chapter 2). Each jurisdiction will need to make decisions about whether and where to maintain LMR coverage.

Jurisdictions will also need to consider when their PSAs may be able to move voice communications onto a PSMB capability. Some states might choose to progressively trial and roll out a PSMB capability as their existing LMR networks come up for renewal. This could reduce the long-term costs of maintaining communications capabilities (where a single network is used) (NSW Telco Authority, sub. 30; Victorian Government, sub. 28). The NSW Telco Authority (sub. 30) anticipates that migration of voice services onto PSMB could commence as early as 2019, provided the appropriate technical standards have been developed and equipment is available and sufficiently reliable.

However, different implementation timetables across jurisdictions could compromise national interoperability. This highlights the need for common national standards that set technical parameters to allow each jurisdiction to adopt interoperable technology when it is ready to roll out PSMB (section 7.2).

The requirements of individual PSAs will also differ across jurisdictions. For example, the Government of South Australia (sub. 29, p. 2) submitted that 'agencies should be able [to] take up the PSMB at a pace that meets their needs and as appropriate technology, services and funding becomes available'.

PSAs will need to take an active role in implementation (section 7.1). They will need to make organisational and cultural changes to make the most of the capability, and work together with other PSAs in developing protocols for sharing information and prioritising users over a shared network. Not least, PSAs will need to make a case for how PSMB will improve public safety outcomes, rigorously evaluate how their use of PSMB achieves such outcomes and innovate. A phased approach to implementation can allow time for these changes to be made smoothly.

A Public consultation

In keeping with its standard practice, the Commission has actively encouraged public participation in this study.

- Following receipt of the terms of reference on 25 March 2015, an advertisement was placed in newspapers in Australia and a circular was sent to identified interested parties.
- An issues paper was released on 20 April 2015 to assist those wishing to make a written submission. A total of 31 submissions were subsequently received (table A.1). These submissions are available online at www.pc.gov.au/inquiries/current/public-safety-mobile-broadband/submissions.
- As detailed in table A.2, consultations were held with a wide range of stakeholders in Australia.
- Technical workshops were also conducted in Sydney and Melbourne to test the proposed approach towards the quantitative analysis. A total of 32 organisations participated (table A.3).

The Commission thanks all parties who have contributed to this study and now seeks additional input towards its final report. The Commission welcomes further submissions to discuss the substance of the draft report, including responses to the information requests, draft recommendations and draft findings.

Table A.1 Submissions[a]

Participant	*Submission number(s)*
ACT Emergency Services Agency	25
Alcatel-Lucent	15
Australasian TETRA Forum (ATF)	4 #
Australian Communications and Media Authority (ACMA)	14
Australian Mobile Telecommunications Association (AMTA)	21
Australian Radio Communications Industry Association (ARCIA)	2
BAI	1
Centre for Disaster Management and Public Safety (CDMPS), APCO Australasia and Victorian Spatial Council	7
Commonwealth Scientific and Industrial Research Organisation (CSIRO)	16
Coutts Communications	20
Department of Communications	23
Emerg Solutions	13
Ericsson	10, 26
Government of South Australia	29
Metropolitan Fire Brigade (MFB) (Victoria)	6
Motorola	12, 31 #
NEC	5
NSW Telco Authority	30
Optus	18
Police Federation of Australia	8
Push2Talk	24
RF Technology	3
Rivada Networks	9, 27
Selex-ES	22
Telstra	19
Victoria Police	17
Victorian Government	28 #
Vodafone Hutchison Australia (VHA)	11

[a] An asterisk (*) indicates that the submission contains confidential material NOT available to the public. A hash (#) indicates that the submission includes attachments.

Table A.2 **Visits**

Participant
Brisbane
Dr Chris Flemming
Queensland Ambulance Service
Royal Flying Doctor Service
Canberra
ACT Emergency Services Agency
Attorney-General's Department
Australian Communications and Media Authority
Australian Competition and Consumer Commission
Australian Federal Police (teleconference)
Australian Maritime Safety Authority
Australian Mobile Telecommunications Association
Department of Communications
Department of Defence
Office of the Hon Malcolm Turnbull (Minister of Communications)
Office of the Hon Michael Keenan (Minister for Justice)
Police Federation of Australia
Hobart
Department of Premier and Cabinet (Tasmania) (teleconference)
Melbourne
Australian Fire and Emergency Service Authorities Council (teleconference)
Australian Radio Communications Industry Association
Centre for Disaster Management and Public Safety (University of Melbourne)
Council of Ambulance Authorities
Country Fire Authority
Department of Economic Development, Jobs, Transport and Resources (Victoria)
Department of Premier and Cabinet (Victoria)
Department of Treasury and Finance (Victoria)
Emergency Management Victoria
Ericsson
Metropolitan Fire Brigade (Victoria)
Motorola
Optus
Paul Harris (Consultant)
Telstra
Trinitas Pty Ltd (teleconference)
UXC Consulting*
Victoria Police
Victoria State Emergency Service

* UXC Consulting was engaged to provide expertise on specific technical issues related to communications infrastructure and technology.

(continued next page)

Table A.2 (continued)

Participant
Perth
Department of Commerce (Western Australia) (teleconference)
Department of Fire and Emergency Services (teleconference)
Department of Parks and Wildlife (Western Australia) (teleconference)
Department of the Premier and Cabinet (Western Australia) (teleconference)
Western Australia Police (teleconference)
Sydney
Centre for International Economics
Robert James (iMediate Consulting)
NBN Co Limited
Nokia (teleconference)
NSW Police Force
NSW Telco Authority (teleconference)
Dr Peter Abelson (teleconference)
Vodafone Hutchison Australia (teleconference)
International
ASTRID (Belgium) (teleconference)
Communications Chambers (United Kingdom) (teleconference)
Rivada Networks (Ireland and United States) (teleconference)

Table A.3 Technical Workshops

Participant
Melbourne
Alcatel-Lucent
Australian Radio Communications Industry Association
Centre for Disaster Management and Public Safety
Department of Premier and Cabinet (Victoria)
Ericsson
Government of Western Australia
Motorola
Robert James (iMediate Consulting)
SA Health
South Australia Police
South Australian Country Fire Service
Tasmania Police
Sydney
ACT Emergency Services Agency
ACT Government
ACT Police
Attorney-General's Department
Australian Communications and Media Authority
Australian Mobile Telecommunications Association
Centre for International Economics
Council of Ambulance Authorities
Department of Communications
Dr Alex Robson
Dr Chris Flemming
Northern Territory Government
NSW Government
NSW Telco Authority
NSW Police Force
Optus
Queensland Ambulance Service
Queensland Government
Queensland Police Service
Telstra
Vodafone Hutchison Australia

B Domestic and international developments in PSMB

This appendix contains summary information on:

- previous reviews of public safety mobile broadband (PSMB) and policy background in Australia (section B.1)
- work underway in key multilateral forums and institutions to harmonise spectrum for delivery of a PSMB capability across international regions, and to develop technical standards for Long Term Evolution (LTE) technology (section B.2)
- summaries of the approach to PSMB in other countries (section B.3).

B.1 Previous Australian reviews and policy background

The need for interoperable public safety agency (PSA) communications has long been on the national agenda. In 2009, COAG endorsed the *National Framework to Improve Government Radiocommunications Interoperability 2010–2020* (COAG 2009). This set guiding principles for aligning narrowband communications systems across the states and territories, including by setting standards for interoperability and moving towards harmonised radio technologies and spectrum use. One of these principles was for jurisdictions to assess common requirements for high speed mobile data interoperability as well as emerging technologies that support increased interoperability. The planned 2015 mid-term review of the framework is underway.

Around 2010, work commenced to identify the need for PSMB and ways to deliver it. Much of this work has focused on the allocation of radiofrequency spectrum. Access to specific frequencies of spectrum is required to wirelessly transmit and receive information, and is a key input to any radio network. Spectrum policy and licensing is the responsibility of the Australian Communications and Media Authority (ACMA).

In 2010, the Australian Government Attorney-General's Department engaged the consultancy Gibson Quai AAS (now called UXC Consulting) to analyse the benefits and costs of providing PSMB under five specific approaches (GQ-AAS 2010). These included establishing a dedicated network (using dedicated spectrum), using commercially provided services, and a combination of both. This work involved building up a detailed picture of PSA requirements (in consultation with PSAs across Australia) and using an engineering model of mobile networks to estimate the costs associated with each approach (excluding the costs of spectrum). It was completed in November 2011. The findings, including demand and cost estimates, were not made public.

The Attorney-General's Department also commissioned a brief report on PSMB spectrum by Access Economics (2010). This drew on the outputs of the study by Gibson Quai AAS Consulting to assess the relative merits of dedicated approaches (including the allocation of spectrum in the 700 megahertz (MHz) band or other spectrum), commercial approaches (a free market approach where PSAs gain access in the competitive market was not considered suitable for technical reasons) and a hybrid approach (using a private PSA network but allowing for commercial arrangements). It found that a fully commercial approach was likely to have the lowest cost, although implementation would be difficult.

In May 2011, the Australian Government established a Public Safety Mobile Broadband Steering Committee (PSMBSC), comprising senior officials representing government agencies, PSA peak bodies and the COAG Standing Council for Police and Emergency Management (Attorney-General's Department 2011). The Committee was tasked with reporting on the most effective and efficient way for Australia's PSAs to obtain a reliable and robust mobile broadband capability that meets their operational requirements. It was also required to work with ACMA to identify a suitable amount of spectrum to meet foreseeable operational needs.

The PSMBSC produced a National Implementation Plan in October 2012, and an Overflow Capabilities Sub Group Final Report in October 2013 (Victorian Government, sub. 28). Neither document was made public. The PSMBSC continued until April 2013, at which point COAG transferred responsibility for PSMB to a group of senior officials (COAG 2013). These officials were tasked with providing advice on establishing an appropriate PSMB capability, in consultation with the COAG Standing Council on Police and Emergency Management. This was to include advice on governance frameworks and the reservation of spectrum.

In November 2014, the Australian Government announced its intention to ask the Productivity Commission to undertake a 'first principles' analysis of the most efficient and effective way of delivering a PSMB capability by 2020 (Turnbull and Keenan 2014).

Parliamentary inquiries have favoured allocating spectrum for PSMB

Policy deliberations have also been informed by two parliamentary inquiries. In November 2011, the Senate Environment and Communications References Committee released an inquiry report on the capacity of communications networks and emergency warning systems during natural disasters. It recommended that the Australian Government 'allocate sufficient spectrum for dedicated broadband public protection and disaster relief (PPDR) radiocommunications in Australia', and that this be provided on the basis of interoperability among PSAs (ECRC 2011, p. vii).

A second parliamentary report was released in September 2013 following an inquiry into spectrum for PSMB conducted by the Parliamentary Joint Committee on Law Enforcement (PJCLE 2013). It found that mobile broadband technology is a significant enabler for improved public safety outcomes, which are in line with community expectations. It also favoured minimising PSAs' reliance on commercial operators for mobile broadband, given the limited resilience and security of commercial networks. The inquiry recommended that 20 MHz of spectrum in the 700 MHz band be allocated for the purposes of a PSMB network, and that proceeds from auctioning other spectrum in that band be used to finance the cost of PSMB spectrum.

Public safety needs are being reflected in spectrum policy

In October 2012, ACMA made an in-principle decision to set aside 10 MHz of spectrum within the 800 MHz band to support the deployment of a PSMB capability. At the time, the Australian Government announced that this spectrum would be subject to a 50 per cent 'public interest' discount for PSAs. ACMA also announced that 50 MHz of spectrum in the 4.9 GHz band would be set aside for exclusive use by PSAs. This was formally licensed in June 2013 (ACMA, sub. 14).

In July 2012, the Premiers of New South Wales, Victoria, Queensland and Western Australia wrote to the Prime Minister to request that 20 MHz of spectrum be allocated for a national PSMB capability, and that part of the proceeds from the auctioning of spectrum in the 700 MHz band be used to construct the PSMB capability (O'Farrell et al. 2012).

In February 2013, all states and the ACT made a joint submission to the Standing Council on Police and Emergency Management and ACMA (ACT Government et al. 2013). In this, jurisdictions expressed concern that 10 MHz of spectrum in the 800 MHz band would not be adequate to meet their operational needs using PSMB. In particular, they noted that it would increase the cost of network construction and operation (relative to using 20 MHz of spectrum) and increase operational risks facing PSAs in mission critical operations.

More broadly, the Department of Communications (2015b) has recently completed a review into Australia's spectrum policy and management framework. Its proposals included:

- replacing the current legislative framework with outcomes-focused legislation that facilitates timely spectrum allocations and greater flexibility of use (including through sharing and trading spectrum)
- requiring public sector agencies to report on their spectrum holdings and allowing them to lease, sell or share spectrum for their own benefit
- reviewing spectrum pricing arrangements to support efficient use and facilitate secondary markets.

State natural disaster inquiry findings on communications

Inquiries into major natural disasters in some states have emphasised the need for a nationally interoperable PSMB capability. Following the Black Saturday bushfires in Victoria in 2009, a Royal Commission found that PSA communications systems were hindered by poor coverage, a lack of interoperability between agencies and insufficient investment in new technologies (VBRC 2010). It drew attention to the use of incompatible radio systems between metropolitan and regional police, and to congestion in PSA radio channels.

The Commission of Inquiry into the 2011 Queensland floods found that interoperability was limited across different parts of the radio network used by Queensland Police at the time, and between PSAs (QFCI 2012). It also found evidence of congestion and 'black spots' on radio networks used by PSAs. The Commission of Inquiry supported the establishment of a statewide digital radio network, and regarded the allocation of broadband spectrum to Australia's emergency service organisations as vital for avoiding congestion on narrowband networks and for achieving interoperability.

B.2 International spectrum harmonisation and technical standards

Spectrum harmonisation has multiple benefits

There are several reasons for international spectrum harmonisation. Radiowaves do not stop at national borders, so harmonisation minimises interference along borders, and also facilitates international roaming. Safety benefits arise, for example, where aircraft and airport communications can be internationally standardised. Harmonising spectrum across countries for specific technologies or applications also means that devices can be produced on a larger scale at a lower unit cost.

The International Telecommunications Union is the lead international forum

The International Telecommunication Union's radiocommunications sector (ITU-R) is the United Nations' specialised agency for information and communication technologies. Broadly, the ITU-R is responsible for the development and maintenance of the international *Radio Regulations*, a treaty-level set of documents which establish an international spectrum management framework. Australia is a Member State of the ITU and conforms to its legal treaties (ACMA, sub. 14).

The ITU-R hosts the World Radiocommunications Conference every 3-4 years to revise the *Radio Regulations*, which include the agreed uses of particular spectrum bands. For spectrum allocation purposes, the *Radio Regulations* divide the world into three regions that loosely comprise — Region 1 of Europe/Africa; Region 2 of the Americas; and Region 3 of Asia and the Pacific (ACMA, sub. 14).

The ITU is working towards harmonising spectrum for PSMB

One of the objectives of the ITU-R is to encourage the harmonisation of spectrum used for particular purposes across countries. To this end, the World Radiocommunications Conference has previously made resolutions about the frequency bands to be used for PPDR in each of the three regions around the world. These suggested bands are not binding on members, as spectrum is often allocated for many years at a time, and governments therefore may not be free to allocate a certain spectrum band to public safety.

In Australia's region (Region 3, Asia-Pacific), the identified spectrum for PPDR as far back as 2003 has been in the 400 MHz and the 800 MHz bands. Since then, countries have been encouraged to undertake further technical and operational studies on a range of matters in relation to the appropriate use of these bands for PPDR. Further consideration of harmonised spectrum for PSMB is on the agenda of the next ITU World Radiocommunications Conference to be held in November 2015 (box B.1).

Box B.1 **PPDR spectrum harmonisation in the ITU**

Public safety agencies (PSAs) have many reasons for using their own communications channels, and have done so historically. Thus, following the development of broadband communications technology and prior to any decisions being made about allocating spectrum for PSA broadband, the International Telecommunication Union (ITU) recognised the opportunity for international harmonisation of spectrum for PSAs. The ITU nominated the benefits of harmonised frequencies as:

- economies of scale and lower costs for implementing specialised systems for public protection and disaster relief (PPDR)
- interoperability of systems on a regional and worldwide basis
- facilitation of local, regional and world planning and coordination activities in spectrum use.

In 2003, a resolution urged governments to consider particular frequency bands for PPDR in each region. In Europe and Africa, certain bands around 400 MHz were considered; in the Americas, frequencies were suggested in the 700 MHz band, 800 MHz band and the 4.9 GHz band; and in Asia and the Pacific, suggested bands included 400 MHz, 800 MHz and 4.9 GHz.

This resolution was updated in 2012 with an acknowledgment that PSA data-traffic demand had increased and would continue to increase, and a recommendation that further study be undertaken ahead of a decision at the 2015 World Radio Conference, both on demand requirements and recommended spectrum bands.

Sources: World Radiocommunication Conference (2003, 2012).

The Asia–Pacific Telecommunity (APT) is the coordinating body for Region 3. The APT Wireless Group has responsibility for various aspects of emerging wireless systems in the Asia-Pacific region, such as promoting harmonisation and facilitating the uptake of new technologies. There are benefits to Australia from spectrum harmonisation:

> The benefits to Australians of the resultant economies of scale are not trivial. For example, the international harmonisation of the 'APT 700 MHz band' – a band used in Australia for 4G services and fast becoming one of the key 4G bands worldwide – has greatly improved the opportunities for economies of scale for network and user equipment operating in that band. (ACMA, sub. 14, p. 4)

Standardising spectrum for public safety can facilitate greater interoperability between PSA officers from different countries, which may be required for emergencies that cross national borders or where PSA officers are sent to assist with an emergency in another country. This is in addition to the benefit of lower hardware costs due to larger-scale production of user devices and equipment.

Many countries are still in the planning stages for allocating spectrum to PSMB — thus, a lot of attention is being given to early movers, who could influence the manufacture of PSA communications equipment. The United States allocated spectrum in the 700 MHz band for public safety use in 2012, and Canada subsequently announced that it would allocate spectrum in the same band. In region 3 (Asia and the Pacific) the ITU has recommended the use of spectrum in the 800 MHz band for public safety (box B.1), however, in 2014, South Korea announced plans to allocate spectrum in the 700 MHz band, in line with the United States and Canada.

There is a broad consensus that LTE will be used for PSMB

Various organisations — from both the telecommunication and public safety sector — have endorsed the use of LTE for PSMB. For example, the 3rd Generation Partnership Project (3GPP) (2013) has noted that:

> With NPSTC [National Public Safety Telecommunications Counsel, USA], TCCA [TETRA and Critical Communications Association, Europe], ETSI Technical Committee [The European Telecommunications Standards Institute] TETRA [Terrestrial Trunked Radio] and other organizations backing LTE there is now a clear global consensus that LTE will be the baseline technology for next generation broadband public safety networks.

The Association of Public-Safety Communications Officials (Australasia) has also endorsed LTE (APCO 2011).

LTE has various enhancements compared to previous mobile technologies

The ITU-R released a report detailing the advantages of LTE for PPDR broadband compared to previous generation mobile technologies (ITU 2014). These include:

- better coverage and capacity, and more reliable services
- simplified, IP-based architecture
- low latency and low packet loss, which are important for real time applications
- greater interoperability due to commercially standardised protocols and interfaces
- better security features and capabilities
- quality of service and prioritisation (enhancements are expected in 3GPP release 14)
- can be flexibly deployed with a wide range of channel sizes/carrier bandwidths.

3GPP plays the lead role in LTE standards development

Each generation of mobile telecommunications technology is defined by the technical standards that apply to it — these set out how hardware and software should be configured in order to be compatible with other technology and meet technical, safety and legal parameters. Various national and regional organisations debate and create standards, including for public-safety related communications. However, given the need for harmonisation, collaboration occurs on an international level between national and regional standards bodies, including 3GPP and others (box B.2). This is true of the technical standards being developed to support the delivery of mobile wireless technologies, including LTE.

Current 3GPP standards in development

In 2014, the 3GPP created a specialist working group responsible for the definition, evolution and maintenance of technical specifications supporting PSA 'mission critical' communications (2015d). Mission critical voice over LTE is expected in Release 13 (which is expected to be frozen, with no further modifications or additions to functionality, in March 2016) (Wendelken 2014). Release 14 will include further work on mission critical video over LTE and mission critical data (3GPP 2015a), see chapter 5, box 5.4 for more detail.

Although LTE is the current standard for mobile broadband communications, the next generation of communications is already being considered. Details of what 5G technology will offer will become available once the relevant 3GPP standards begin to take shape (ACMA, sub. 14).

Box B.2 **3rd Generation Partnership Project (3GPP)**

3GPP unites six telecommunications standard development organisations[a] to produce reports and specifications that define 3GPP technologies — for example to ensure that technology is compatible with previous and future user equipment. 3GPP has done significant work on the technical standards and technologies for Long Term Evolution (LTE), including technical work to produce enhancements to the LTE standard to support public safety applications.

Release 8 (frozen[b] in 2008) marked the beginning of LTE standards, introducing a new radio interface and core network, and enabling higher data speeds and lower latency. Features included a flat radio network architecture and an all Internet Protocol core network.

Release 9 (2009) introduced a number of refinements and new features including self organising networks, location services and a more efficient way to deliver the same multimedia content to multiple destinations.

Release 10 (2011) provided a substantial uplift to the capacity and throughput of the LTE system and also took steps to improve the system performance for mobile devices located at some distance from a base station. It also included carrier aggregation, allowing the combination of up to five separate spectrum bands to enable higher bandwidths.

Release 11 (2013) included provisions for device-to-device communications, enhancements to carrier aggregation and the introduction of new frequency bands.

Release 12 (2015) was the first to include major work on the use of LTE for critical communications, with public safety features such as direct mode communications and system enablers for group call and mission critical push-to-talk.

In addition to the 3GPP, there are other umbrella standards organisations that seek to promote international harmonisation. For example, the Global Standards Collaboration created a Task Force on Emergency Communications that, in July 2014, presented a draft report collating the standards relevant to public safety across key nations.

[a] They are: the Association of Radio Industries and Businesses, Japan; The Alliance for Telecommunications Industry Solutions, USA; China Communications Standards Association; The European Telecommunications Standards Institute; Telecommunications Standards Development Society, India; Telecommunications Technology Association, Korea; Telecommunication Technology Committee, Japan.

[b] Frozen means no further modifications or additions to functionality: only essential corrections can be made following freezing.

Sources: 3GPP (2015c); ACMA (sub. 14); Brydon (2012); GSC (2014).

B.3 Approach to PSMB in other countries

A diverse range of approaches is used to deliver PSMB internationally. While some countries have made significant progress in planning for a PSMB capability, there is currently no network in place which provides PSAs with a ‘public safety grade’ mobile broadband capability. While some countries are planning to construct dedicated mobile broadband networks for their PSAs, all are expected to make significant use of existing commercial infrastructure and expertise.

United States

The US Government is planning to build and operate a nationwide LTE network exclusively for PSAs. A government authority (FirstNet) was established in 2012 to manage the delivery and operation of the network. Federal funding (US$7 billion) and dedicated spectrum (20 MHz in the 700 MHz band) has been set aside for this project.

Policy context

The original US Government plan to deliver a PSMB capability involved using commercial service providers (Telstra, sub. 19). To facilitate this, the Federal Communications Commission auctioned 10 MHz of spectrum in the 700 MHz band (known as the 'D block') with requirements that it be made available to PPDR users under certain circumstances (but could be used by a commercial provider at other times).

However, commercial mobile providers did not purchase this spectrum, and subsequently the US Government decided to allocate it for a public safety network (combined with 10 MHz of spectrum already licensed to public safety), and created FirstNet. There were two key motivations for the establishment of FirstNet. The first was that a lack of interoperability had hampered the overall effectiveness of public safety operations during various emergency incidents — including the terrorist attacks in September 2001 and Hurricane Katrina in 2005 (USGAO 2015). The second was concerns that commercial mobile networks were not satisfactory for public safety needs (FirstNet 2015a).

FirstNet is responsible for ensuring the network provides a single interoperable platform for public safety communications, and is delivered cost-effectively, including through leveraging existing infrastructure and assets (Essid 2012; FirstNet 2015a).

A recent report identified challenges with the implementation of the project — including the approach to procurement, conflicts of interest, slower than expected progress in some areas, and concerns that the US$7 billion in federal funding will be insufficient to facilitate the deployment and maintenance of the network (USGAO 2015). This report also noted that estimates on the costs of constructing and operating the FirstNet network over the first 10 years range from US$12 – 47 billion.

Governance and institutional arrangements

Provision of a PSMB capability in the United States has been centralised at the national level (Moore 2015). FirstNet has its own Board of Directors which includes representatives from the Federal Government (Attorney-General, Secretary of Homeland Security, Director of the Office of Management and Budget), and other representatives from PSAs and local, state and federal government; and the wireless industry (FirstNet 2015a).

FirstNet is expected to become a self-sustaining business model. While FirstNet's business plan is still taking shape, it is envisaged that revenues will come from user fees and agreements with contractors that will leverage the value of any excess network capacity it has (FirstNet 2015a).

Cooperation and consultation between different levels of government is evident in the approach. The law that established FirstNet requires it to consult with federal, state, tribal and local public safety entities to ensure that the network is designed to meet each state's needs. To streamline these efforts a single point of contact was established by the Governor in each state. FirstNet began these consultations in 2013 and they are ongoing (FirstNet 2015a).

Individual states will have a choice to 'opt in' or 'opt out' of the project — but either way they must deliver a PSMB capability that meets minimum technical standards, and is interoperable with FirstNet's network. Once FirstNet has completed its Request for Proposal process for building, operating and maintaining the network, a state has 90 days to agree to allow FirstNet to construct a radio access network in that state, or notify its intention to deploy its own. (The Federal Communications Commission will either approve or disapprove a state plan.)

Network design features

FirstNet is seeking comprehensive network and service solutions covering all US states, territories, and tribal nations. At the network level, this includes:

- the deployment and provisioning of a nationwide core
- all radio access network components for 'opt-in' states
- backhaul, aggregation and national transport networks, and data centres
- deployable capabilities.

FirstNet's network planning and design is an ongoing process. In April 2015, FirstNet released a draft Request for Proposal which outlined its current thinking on coverage objectives, minimum technical requirements and performance standards (FirstNet 2015b).

- Coverage — Minimum coverage objectives for each state have been established following consultation. Coverage is defined as a minimum of 768 Kbps downlink and 256 Kbps uplink (at the cell edge with 50 per cent loading). Coverage requirements must meet or exceed an 'average downlink throughput per square mile' data rate — differentiated depending on the population density and other characteristics of different geographic regions.
- Minimum technical requirements — The Federal Communications Commission approved minimum technical standards for achieving nationwide interoperability for PSMB which FirstNet is required to abide by (FCC 2012). These include complying with 3GPP, and open, non-proprietary standards.
- Performance standards — Salient features include: annual end-to-end user service availability of 99.9 per cent; priority and pre-emption mechanisms which can be

managed statically and dynamically by public safety users; and integration of radio access networks of states that 'opt out'.

Some of the objectives outlined by FirstNet are intended to be broad enough to allow potential contractors to find innovative ways to meet or exceed these standards (FirstNet 2015d). In designing its network, FirstNet is also required to seek to leverage existing telecommunications infrastructure and assets. This includes exploring public/private partnerships that can help support and accelerate the creation of the network.

From a service application perspective, FirstNet's initial focus is to support mobile data services, with mission critical voice communications expected to be integrated in the coming years (USGAO 2015). In the meantime, US states are expected to continue to invest in their land mobile radio (LMR) networks, although these are eventually expected to interoperate with the FirstNet network (FirstNet 2015a).

Supporting analysis

Some publicly available analysis and studies were undertaken prior to the creation of FirstNet. The Federal Communications Commission undertook work in this area in 2010.

A technical analysis found that a dedicated network with access to 10 MHz of spectrum in the 700 MHz band would provide more than the required capacity for day-to-day public safety communications, and for a range of emergency scenarios it considered (FCC 2010b). While this network it would not cater for the largest emergencies, it was found that access to another 10 MHz of spectrum would still be insufficient in these cases. Accordingly, priority access and roaming on commercial networks was noted as critical to providing adequate capacity in extreme situations, and more cost-effective.

A broadband network cost model developed by the Federal Communications Commission indicated that PSAs could leverage the deployment of 4G commercial wireless networks to greatly reduce the overall costs of constructing their nationwide broadband network (FCC (2010a). Specifically, it found that an approach which leverages off existing commercial infrastructure would save more than US$25 billion (US$9.2 billion in construction and US$15-20 billion in operation and maintenance) over the first ten years.

In the lead up to the allocation of the 'D block' spectrum for public safety, a study by Ford and Spiwak (2011) considered whether additional 'D block' spectrum should be assigned to public safety or auctioned. It found that assignment to public safety would provide at least US$3.4 billion more in social benefits than it if were auctioned. This study did not attempt to quantify the costs of developing a dedicated PSMB network, or the benefits of public safety use of spectrum, noting that:

> Perhaps the most daunting, yet relevant, question regards the social benefits of 'public safety.' *Such benefits are real but difficult to quantify* and, absent immediate crisis, prone to be undervalued. … For the moment, we choose to set aside the quantification of the benefits of an

additional 10 MHz of spectrum for public safety, looking instead at the cost side of equation. (2011, p. 10)(emphasis added)

Current status

FirstNet expects to issue the final Request for Proposal in late 2015 (Jackson 2014).

United Kingdom

The UK Government is currently in the process of procuring a new Emergency Services Network to fully replace its current narrowband network for PSAs by 2020. This project involves contracting with commercial networks to deliver a PSMB capability, without the allocation of dedicated spectrum for PSA use.

Policy context

Since the early 2000s, a single communications network has provided mission critical voice and narrowband data services to PSAs across the United Kingdom. This network, which is based on TETRA digital technology, covers around 99 per cent of the UK landmass and provides some underground and air-to-ground coverage (PA Consulting Group 2013). It is operated by Airwave, a private-sector company, under contracts that begin to expire in September 2016 and will be fully expired by 2020 (UK Home Office 2015a).

The Airwave network does not have sufficient capacity to support many data applications, and PSAs have expressed concerns about the quality of service offered over commercial mobile networks (Analysys Mason 2012; PA Consulting Group 2013). Although PSAs have made increasing use of commercial mobile broadband in the United Kingdom, most do not rely on it for mission critical functions (Cole and Hawker 2014).

Since 2012, the UK Government has sought to move to a single integrated network to provide mobile voice and broadband data services to PSAs. This new Emergency Services Network is intended to replace the existing Airwave network over the period 2017–2020, and ultimately provide mobile broadband services to an estimated 250 000 operational staff across over 400 national and local government agencies (UK Home Office 2014).

Cost is widely seen as a major motivation for moving towards an integrated mobile broadband solution by 2020: contracts with Airwave for the network and related services total around £400 million per year (SCF Associates 2014). The UK Government recently announced that it expected the new Emergency Services Network to save around £1 billion over the next 15 years (UK Home Office 2015a).

Governance and institutional arrangements

The provision of a PSMB capability has been centralised at the national level. The UK Home Office (through its Emergency Services Mobile Communications Programme) formally commenced a tender process in April 2014, in which procurement was divided into four contracts or 'lots':

- lot 1 — delivery partner (program management, including procurement of end-user devices and the transition of PSA users on to the new network)
- lot 2 — user services (provision of end-to-end systems integration, management of user accounts and provision of user services)
- lot 3 — mobile services (provision of a national mobile network by a network operator to the resilience and other standards required by PSAs)
- lot 4 — extension services (extension of mobile network infrastructure beyond the lot 3 area) (UK Home Office 2014, 2015b).

Companies were generally permitted to bid for multiple lots, with the exception of the delivery partner tender (which must have an independent supplier) (UK Home Office 2014). The extension services tender was cancelled early in the process (after four of the five bidders pulled out) (Clemons 2015), with changes made to the coverage requirements of the mobile services tender (Skinner 2015).

The UK Home Office (2014) estimated the value of all contracts (excluding extension services) at £380 million to £870 million, of which mobile services were estimated at £200 million to £530 million. Each contract was anticipated to have a duration of 5 to 6 years. After this, the mobile and user services contracts are to be re-tendered (Shipley 2015).

The main procurement process is being supplemented by a range of other initiatives.

- A separate contract is expected to be signed with the winning bidder for mobile services, covering 'business critical' mobile services provided on a wholesale basis (at agreed prices) (SCF Associates 2014).
- Procurement processes are underway for the provision of user devices, vehicle installations, an 'air to ground' network, and upgrades to control rooms (UK Home Office 2015b).
- An 'extended areas services' project to expand the reach of mobile networks has been announced, though few details are available publicly (UK Home Office 2015b).

Network and service features

Little information is publicly available on the exact service features to be provided by the mobile services contract (lot 3). Official procurement documents refer to 'an enhanced mobile communications service with highly available full coverage' (UK Home

Office 2014). Other official sources state that the new network would need to provide public-safety functions and end-to-end security (Shipley 2015), and a high level of coverage (98 per cent by population on an in-building basis, and 90 per cent geographic coverage) (UK Home Office 2015b).

In addition, the network is to run on LTE technology and adopts 3GPP international standards. Since standards to support public-safety voice requirements are not yet in place (chapter 5), the Home Office is prepared to access pre-standards (proprietary) technologies on the basis that these are upgraded to comply with future international standards (Shipley 2015).

A report by SCF Associates (2014) points to other requirements, including the same or greater resilience as the Airwave network (with 5 to 7 days of power supply backup at key sites), the provision of public safety features for data and voice (such as group call, push-to-talk and direct-mode communications), and priority of emergency services users over commercial customers on the network. To meet these, some modification or 'hardening' of commercial networks is anticipated.

In addition, interfaces with the Airwave network are to be implemented at the control-room level to support the gradual transition of PSA users onto the mobile broadband network (SCF Associates 2014).

Supporting analysis

A strategic business case for the Emergency Services Network was prepared by the UK Home Office, and approved in 2012 (WYFRA 2013). User requirements were planned to be finalised by the end of 2013 (Shipley 2013). However, neither document appears to have been made public.

It has been reported that four business cases were examined:

- continuation of the Airwave network with the addition of advanced data capabilities
- building a new TETRA (narrowband) network
- building a new LTE network to public safety specifications (using dedicated spectrum)
- forming contracts with commercial LTE network owners to deliver services to PSAs under specific service-level agreements (Clemons 2015).

Sources indicate that the commercially procured service was estimated to deliver the best value for money (SCF Associates 2014) — with a cost in the order of £3.7 billion, around £1 billion less than the first two TETRA-based options, and at least £3 billion less than building a new LTE network (Clemons 2015).

Current status and next steps

The tender process formally commenced in April 2014 with the expected completion by April 2015 (UK Home Office 2014). This has not yet occurred; a contract is now expected to be awarded in October 2015 (Shipley 2015). The service is expected to commence in July 2017, with public safety users transitioning on to the new network by February 2020 (Shipley 2015).

In February 2015, eight bidders were invited to progress to the negotiation stage of procurement: four for delivery partner (lot 1), two for user services (lot 2) and two for mobile services — EE and Telefónica (lot 3) (UK Home Office 2015a). In June 2015, Telefónica formally withdrew from the process (Skinner 2015).

Canada

The Canadian Government has set aside 20 MHz of spectrum in the 700 MHz band for the development of a public safety broadband network. Interoperability across the border with the United States has been a key consideration, and this is the same spectrum band as reserved for public safety in the United States. The expectation is that provinces and territories will be able to choose whether to construct a dedicated mobile broadband network using this spectrum, or to procure services from commercial carriers.

Policy context

The Canadian Government has been consulting with stakeholders on the potential allocation of spectrum for PSMB since at least 2011. In that year, emergency management ministers from the provinces and territories recommended to Industry Canada (the spectrum regulator) that 20 MHz of spectrum in the 700 MHz band be set aside for public safety (Public Safety Canada 2012).

In 2012, an announcement was made to set aside 10 MHz in the 700 MHz band for public safety, with further consultation to be undertaken on adding another 10 MHz (Public Safety Canada 2012). The need for interoperability across the United States border (along which much of Canada's population resides) was prominent in consultations (Industry Canada 2012).

The allocation of the additional 10 MHz was announced as part of the 2015 Canadian Government budget, bringing the total allocation for public safety to 20 MHz (Government of Canada 2015). The Government also announced that it would provide C$3 million over two years from 2016-17 to take initial steps to establish a Public Safety Broadband Network (Government of Canada 2015).

Governance and institutional arrangements

While governance arrangements are yet to be finalised, there are indications that the provinces and territories will have primary responsibility for funding and providing PSMB.

A national nonprofit entity is to be established to develop national standards for interoperability and enter into roaming agreements with commercial networks and FirstNet in the United States (Public Safety Canada 2012, 2013). It will also hold the licence for the spectrum and be responsible for constructing, maintaining and operating a core network that would allow for linking networks in each province and territory.

The spectrum would be sub-licensed to a 'regional service delivery entity' in each province and territory (Public Safety Canada 2012, 2013). These entities would then deploy a mobile broadband capability, using either the dedicated spectrum, commercial mobile services, or a combination of the two. In doing so, they would be required to adhere to national standards for interoperability across provinces and with the United States. They would also be required to fund their networks by establishing cost recovery models for services provided to users.

A separate process is underway between Canada and the United States to harmonise their prospective public safety broadband networks and to establish protocols to minimise interference in border areas (NPSTC and CITIG 2015).

Network and service features

Few network design features have been agreed on to date. An exercise conducted in 2013 to identify network architecture requirements (in consultation with PSAs, government officials and other stakeholders) indicated that the network(s) would be based on LTE technology. It also set out expectations of a high level of security and resilience (including no single points of failure and hardening of network equipment), as well as the prioritisation of public safety traffic during periods of network congestion (CSS 2013).

It is likely that each province or territory will have its own core network, and these will be linked to a national core network to facilitate communications across jurisdictions (CSS 2013; Fournier 2015). This is to be supported by roaming agreements that allow users to access their information when on another network, as well as arrangements to allow federal PSAs to access the networks in each province or territory (CSS 2013).

The network architecture exercise envisioned that roaming agreements would be established with commercial carriers to improve geographic coverage, and that deployable broadband communications infrastructure would be used to respond to incidents in isolated areas where it is not feasible to provide permanent radio coverage (CSS 2013). These systems will likely use satellite backhaul or operate on a standalone basis (that is, not directly connected to wider networks).

In addition, there are likely to be gateways between PSMB networks and existing LMR networks used to provide mission critical voice services (CSS 2013). These narrowband networks are expected to continue for the foreseeable future.

Supporting analysis

In 2011, the Centre for Security Science (part of Defence Research and Development Canada) conducted a technical assessment of the 700 MHz spectrum requirements for mobile broadband data communications (CSS 2011). In consultation with PSAs and other stakeholders, it developed several incident scenarios to assess data throughput and application requirements. The analysis found that PSAs would need access to more than 20 MHz of spectrum to conduct missions during commonly occurring major emergency situations.

Current status and next steps

Consultation on the policy, technical and licensing framework for the public safety spectrum is ongoing (Industry Canada 2012). The financing, structure and governance of the Canadian network are yet to be finalised, and the spectrum has not yet been licensed or priced (Solomon 2015). Work still needs to be done to develop standards and address network sharing, dynamic prioritisation, spectrum coordination and cross-border interoperability (Fournier 2015).

A permanent network is not expected to be in place for another three to five years, however, several initiatives are underway across Canada to construct test networks (using LTE technology in the public safety spectrum band) (Solomon 2015). For example, Industry Canada is testing a network in the 700 MHz band in Ottawa, which involves evaluating and testing equipment, software and applications. Work is also underway to establish a national capability for testing deployable mobile cells, which are intended to be used in remote areas or when conventional networks are damaged (Fournier 2015).

South Korea

In July 2014, the South Korean Government announced plans for SafeNet, a PSMB network using LTE technology, to be deployed by 2017. It was subsequently announced that 20 MHz in the 700 MHz bandwidth had been allocated for this purpose (LTE-Applications 2014).

Policy context

On 16 April 2014, the Sewol ferry capsized off the South Korean coast, killing 304 people, most of whom were high school students. According to the National Task Force for Korea Public Safety Broadband Network, the event ‘brought attention to the urgent need for establishing a nationwide public-safety broadband network for sharing information and communicating among public-safety agencies' (Zilis 2014).

Rescue and response efforts were hindered by a lack of communications interoperability from responding agencies. At the time, PSAs each operated separate voice networks on a variety of frequency bands, using a variety of technologies that were not interoperable with each other (Zilis 2014).

Network design features

SafeNet will be a private, dedicated network for approximately 200 000 users from 324 agencies including police, fire, Coast Guard, military, provincial administrative offices, electricity, gas and forest services. The network is intended to provide full geographical coverage for day-to-day as well as mission critical usage. Although the network will support both voice and data services, it is envisaged that legacy networks will be retained as backup (Kim 2015).

Governance and institutional arrangements

To date, planning for SafeNet has largely been overseen by the Ministry of Security and Public Administration. Additionally, the Ministry of Science, Information and Communication Technology, and Future Planning has made recommendations in relation to the choice of technology, frequency band and procurement method. It is envisaged that a new agency, the Ministry of National Security, will soon be established and charged with national security matters, including the network (Zilis 2014).

Although SafeNet is a dedicated network, it will leverage existing commercial infrastructure, including commercial backhaul and base station infrastructure. It is estimated that the network will cost US$840 million (Kim 2015).

Current status and next steps

To date, the government has conducted a Request for Proposal process, as a result of which LG CNS was selected to create an information strategy plan. This plan addresses expected cost, network site specifics and how a vendor will be chosen (LTE-Applications 2014).

The network will be rolled out in phases. In the first phase, the network will be piloted in selected areas in the Gangwon Province, including Pyeongchang, where the 2018 Winter Olympics will be held. Rollout of the network will focus on rural areas first, which, unlike urban areas, currently do not have a unified network. In the second phase, the network will be extended to cover other provinces, and phase three will cover metropolitan cities. It is envisaged that the third phase will be completed in 2017 (Kim 2015).

New Zealand

PSAs in New Zealand — and police in particular — have started using mobile applications, tablets and smartphones on a wide scale. However, these are mainly standard commercial services delivered over commercial carrier networks, rather than a 'public safety grade' service.

Policy context

Mobile broadband has already been taken up by PSAs in New Zealand, although LMR voice systems remain in extensive use. In 2013, New Zealand Police signed a contract with Vodafone for mobile broadband services as part of its Policing Excellence program. The 10-year contract includes the provision of smartphones and tablets in addition to mobile broadband services (Key 2013). The total cost of the rollout was estimated at NZ$159 million.

In 2014, the St John Ambulance service started rolling out an 'electronic patient report form' project. This involved equipping officers with mobile tablets so that paper forms can be replaced with electronic records, and installing Mobile Data Terminals in ambulances to allow officers to communicate their status during a response and their availability to accept jobs (Paredes 2014a). The project will allow ambulances to collect and share more 'vital sign' information with hospitals while patients are in transit.

Network and service features

The New Zealand Police service mainly relies on Vodafone's commercial network for mobile broadband. As far as the Commission is aware, the contract with Vodafone does not involve the delivery of a public safety grade service — that is, there are no special arrangements to give police additional coverage, priority or network reliability over what is delivered to other customers on the network.

As of December 2014, around 14 000 mobile devices had been deployed to police across New Zealand (Woodhouse 2014). In addition, a Mobility Innovation Lab and Experience Centre has been established to develop and test new mobile broadband applications and technologies to support policing operations (Paredes 2014b).

Supporting analysis

A review of the Policing Excellence program found that mobile broadband has allowed police officers to use mobile devices to access email and maps, take photos, share documents and make phone calls. This includes:

- accessing police-specific applications and databases (relating to people, vehicles and locations) from the field

- accessing real-time information on police operations through a Mobile Responder application
- making calls to a dedicated number to dictate information about an incident (which is then transcribed and stored in a database) (New Zealand Police 2014; Paredes 2014b).

These applications have been credited with improving decision making, access to information, officer safety and situational awareness, while reducing time spent on paperwork and data entry. In the 12 months to June 2014, mobile broadband has allowed police officers to make an estimated 2.9 million database queries, gain an additional 30 minutes per officer per shift (totalling 520 000 hours per year), and reduce demands on voice radio networks (New Zealand Police 2014). The productivity benefits over the life of the 10-year contract with Vodafone have been estimated at NZ$305 million (Vodafone 2013).

Belgium

Summary of the approach

Since 2014, a mobile broadband service — Blue Light Mobile — has been available to PSAs across Belgium.

Blue Light Mobile is operated by ASTRID, a government owned entity responsible for emergency communications in Belgium. Blue Light Mobile provides PSAs with access to Belgium's three commercial carriers, as well as select carriers from adjacent countries in border areas. To achieve multiple carrier access, ASTRID acts as a mobile virtual network operator and enters into international roaming agreements with the relevant commercial carriers. PSAs then access the Blue Light Network by using an internationally registered SIM card, affording them international roaming status (and access to all carriers) inside Belgium.

Blue Light Mobile is not considered a mission critical service, as there is no guaranteed access for PSAs during periods of congestion, nor an ability to seamlessly roam across networks. However, Blue Light Mobile offers an enhanced quality of service relative to commercial best efforts, with PSAs receiving priority once they have accessed the network, increased reliability due to coverage overlap between carriers, as well as some enhanced security options.

Policy context

Since 1998, ASTRID has supplied the Belgian police, fire and ambulance services with national radio communications, and paging and dispatch services. The ASTRID radio network operates on the TETRA standard in the 380-400 MHz frequency band (which is exclusively reserved for emergency and security services across Europe). The network achieves complete in-vehicle geographical coverage of Belgium (ASTRID 2011b).

In 2012, ASTRID initiated a study into how an efficient mobile broadband data network could be established across Belgium. This study was driven in part out of concern that PSAs were seeking individual PSMB solutions from different commercial cellular operators, fragmenting systems and applications across PSAs. The study concluded that a commercial solution was the most viable option as:

- EU-wide harmonised spectrum for PPDR is not yet available
- immediate budgetary constraints ruled out a fully dedicated solution (TETRA Applications 2012).

Use of commercial networks is seen as a temporary solution. It achieves some short term goals (such as providing a common PSMB capability to all PSAs) while simultaneously acting as a form of 'pilot' upon which the business case for a fully dedicated PSMB network can be based.

Governance and institutional arrangements

The Blue Light Mobile network is operated by ASTRID, a company established under Belgian public law that is jointly owned by the federal government and Belgian towns and provinces (ASTRID 2011c). Under the law, ASTRID is required to establish, run, maintain and implement a radio communications network for voice and data transmissions for Belgian emergency and security services, amongst others.

Network design features

Roaming is enabled via an internationally registered ASTRID SIM card, as ASTRID has negotiated international roaming agreements with the relevant commercial networks. The SIM cards have a 'preferred' or default network, and will switch to other commercial network whenever coverage is lost (ASTRID 2011a; TETRA Today 2014). Each organisation using the Blue Light network can individually choose the preferred network to which their devices will connect (ASTRID 2014b). However, roaming between networks is not seamless, with handover from one network to another requiring disconnection, searching, reconnection and authentication with the new network, a process that can take up to two minutes.

Network reliability is enhanced through the use of multiple carriers providing coverage overlap, although no hardening of the commercial networks (such as increased battery back-up or civil works) has been undertaken. The TETRA network (which covers 100 per cent of Belgium's landmass) is used as a back-up in the event that all commercial 3G networks are saturated or defective. Switching to TETRA is not automatic and requires manual input from the user (ASTRID 2014b).

While not a mission critical service, there are network elements which provide for a quality of service beyond a commercial 'best efforts' basis. Once access to the network is achieved, PSA users receive a measure of priority through a 'guaranteed minimum bitrate', and commercial customers are allocated any residual capacity. This minimum bitrate is set in advance (that is, it cannot be varied in real-time) and is only available on the user's designated primary network (ASTRID 2014b). Further, security is enhanced through the use of a Virtual Private Network between a common ASTRID database and the PSAs. For applications and data stored outside of ASTRID's common database, security features (such as encryption) are the responsibility of each agency (ASTRID 2014a).

Supporting analysis

The Commission is not aware of any studies evaluating the costs and/or benefits of a PSMB capability in Belgium. However, data and experience gathered from Blue Light Mobile will form the basis of a business case for any future dedicated PSMB network.

Current status and next steps

Blue Light Mobile is fully operational, with police, fire and ambulance all using the service. Police have proved to be the heaviest users. In the short term, PSAs are seeking additional functionality to increase reliability, such as guaranteed access. In the long term, Blue Light Mobile is a temporary solution on the path to a fully dedicated national PSMB network.

Finland

Summary of the approach

Finland is following a staged, incremental approach that combines the current LMR network with new broadband capability provided by commercial operators. Similar to the Belgian model, PSAs will be able to roam across commercial mobile network operators to ensure access to the best available connection. A data mobile virtual network operator has been deployed by Athonet and Airbus Group. This will allow secure, non-critical mobile broadband communications, and critical voice and messages will continue to be sent via the LMR (narrowband) network, possibly for another 15 or 20 years. Only when broadband service availability and reliability meets PSA mission critical requirements will LMR networks be dismantled, and this, too, will be a staged process beginning in rural areas when the narrowband network spare parts stock runs out (ATF, sub 4; Airbus Group 2015).

Policy context

The five-step plan to implement a PSMB capability for PSAs is being led by VIRVE, the operator of Finland's LMR network. The transition pathway begins in the next 5-10 years and will deliver a government-controlled hybrid solution (of dedicated and commercial LTE networks) when the current TETRA network reaches the end of its life around 2030 (Vinkvist, Pesonen and Peltola 2014).

C Quantitative methodology and results

C.1 About this appendix

This appendix documents the quantitative analysis undertaken by the Commission as part of assessing indicative costs of delivering a PSMB capability via different delivery options.

The quantitative approach discussed in this appendix is limited to assessing the relative cost effectiveness of different options for delivering a PSMB capability and identifying the key drivers of cost differentials between options. That is, it aims to develop cost estimates for different delivery options for the purpose of 'screening', rather than setting out a detailed business case for a PSMB capability per se.

In particular, the quantitative analysis does not provide insights into the benefits or risks of a PSMB capability or the extent to which these benefits or risks vary between delivery options. Moreover, the institutional and regulatory arrangements required to deliver a PSMB capability via any of the options are outside the scope of the quantitative analysis. (These issues are discussed qualitatively in chapter 7.)

The Commission's quantitative approach was discussed at two workshops, one in Melbourne on 23 June 2015 and the other in Sydney on 25 June 2015. Participants included representatives from public safety agencies (PSAs) and academia, commercial mobile carriers, equipment providers, telecommunications industry experts and government officials. The Commission also conducted one-on-one meetings with selected participants to validate some of the technical inputs.

Feedback and comment is sought on the inputs and assumptions used in this appendix, with a view to finalising these matters for the final report. The Commission will make the computer files to run the quantitative analysis publicly available for the final report.

The structure of this appendix is as follows.

- The core framework is discussed in sections C.2–C.5.
- The parameters for the analysis and their calibration are discussed in section C.6.
- The results are discussed in section C.7.
- Sensitivity analysis is discussed in section C.8.
- Costs that are outside the scope of the quantitative analysis are set out in C.9.

C.2 Overview of the quantitative framework

The objective of the quantitative analysis is to identify indicative cost differences between different options for delivering a PSMB capability. The choice of framework and methodology has been driven by its suitability for this purpose.

In particular, the fit-for-purpose framework and methodology is designed to:

- be capable of constructing representative mobile networks for different options in a manner that yields broadly comparable outputs
- have sufficient descriptive power, so as to allow different options to be characterised differentially within the framework
- calculate the incremental costs of a specified network in such a way that preserves relative cost magnitudes between options
- identify key drivers of cost differences, particularly those arising from differences in:
  - the geographical footprint of the dedicated portion of the network
  - the number of mobile carriers involved
  - arrangements relating to PSA traffic overflow
- allow key assumptions and parameter values to be varied
- cover a time horizon sufficient to capture network rollout, upgrades and technology replacement cycles.

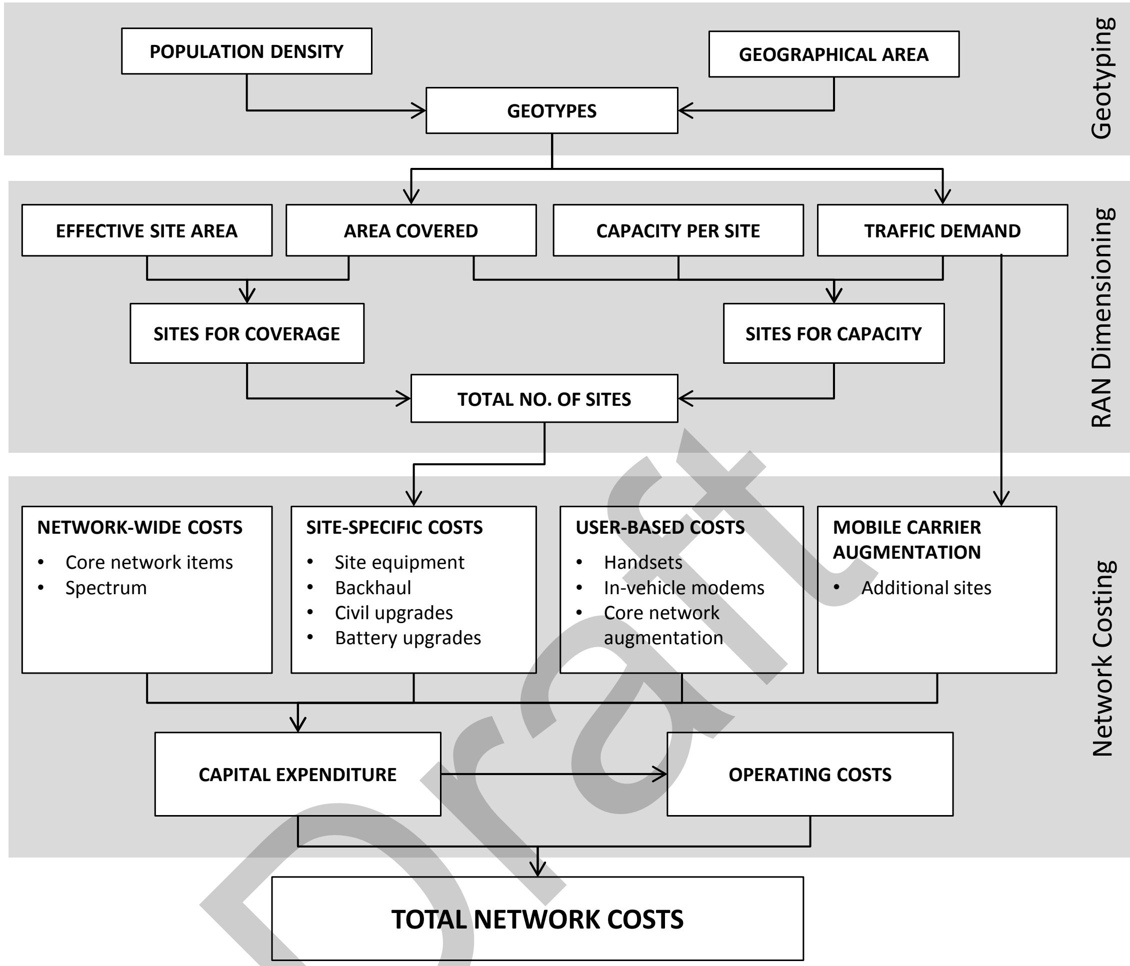
Importantly, the framework and methodology applied is not designed to necessarily:

- produce precise estimates of the costs of a particular option, or individual components
- describe what the architecture of a PSMB network would look like in practice
- identify the optimal mix of inputs for delivering a PSMB capability.

An overview of the framework for quantitative evaluation is depicted in figure C.1. The framework can be described as a bottom-up approach, which is generally viewed as preferable for calculating investment costs (Brinkmann et al. 2007; Smura 2012). The approach taken is also modular, in the sense that the overall framework can be subdivided into smaller distinct parts, each of which is discussed in further detail below.

- The geotyping module links geographical areas to demand characteristics, via the assignment of geotypes (section C.3)
- the radio access network (RAN) dimensioning module determines the number of sites required to provide coverage and meet capacity requirements (section C.4).
- the network costing module calculates selected capital expenditure and operating costs associated with delivering PSMB (section C.5).

Figure C.1 **Framework for evaluating costs**



Since the early 1990s, techno-economic modelling has been used to analyse and compare the economic feasibility of emerging telecommunications networks and services (Smura 2012). The objective is to compare technical options to determine the most cost-effective solutions and to identify the parts of the network that contribute most to overall costs. The modelling is multidisciplinary in combining engineering and economic methods.

The framework applied in this study has similarities with this type of approach and is in part based on other models of mobile networks in the literature (Analysys Mason 2015; GQ-AAS 2010, 2011b, 2011c). However, the modelling framework applied here is adapted to the specific nature of this study. It should be noted that certain costs are not accounted for as part of the quantitative analysis. These are discussed in greater detail in section C.9.

C.3 Geotyping

A key step in evaluating the cost of delivering a PSMB capability involves identifying how demand for and supply of PSMB services would vary over Australia's geographic area. This study adopts a 'geotyping' approach to identifying the demand and supply characteristics of geographical areas. Accordingly, Australia's geographic area is divided into classes or 'geotypes', whereby all areas with the same geotype have the same characteristics on average. Specifically, areas within a geotype class are deemed to share similar demand profiles for PSMB services and hence require similar network solutions to meet this traffic.

Why use geotypes?

A site-by-site approach would be data intensive

One approach to this task is to dimension the network on a site-by-site basis, taking into account the unique traffic and geographical characteristics of local areas. However, such an approach would have extremely high informational requirements, including comprehensive geographical data and robust traffic forecasts. It is also unlikely that this level of detail is necessary for understanding the relative cost of different options (as opposed to the magnitude of costs per se).

A benchmarking approach could overestimate costs

Another approach would be to use the networks of mobile carriers as a benchmark for the architecture of a PSMB. However, a limitation of this approach is that mobile carrier networks are designed to meet commercial traffic, which is likely to be considerably greater than PSMB traffic (due to a greater number of users), especially in metropolitan areas. As a result, a benchmarking approach risks significantly overestimating the total number of sites and therefore the cost of delivering a PSMB capability via any option. Additionally, under a benchmarking approach, it is difficult to identify the key drivers of costs, as many of the key cost items are derived from a 'top down' analysis.

The approach taken is fit for purpose

Instead, this study uses geotypes for the purpose of describing areas of similar demand and supply characteristics. One limitation is that an approach relying on averaging across 'geotypes' does not take into account the idiosyncrasies of specific geographic areas. Nevertheless, the specified characteristics are representative of the geotype class as a whole, as variances within the geotype class are assumed to counterbalance each other. For example, an especially rugged geographic area that requires more cells for coverage will be counterbalanced by flatter areas that require fewer.

How are geotypes assigned?

It is first necessary to determine the basis on which geographical areas are assigned a geotype. This has been done with reference to two key criteria.

The first is that the specification of geotypes must be implementable, in the sense that there must be an empirical basis for mapping geographical areas within Australia to a geotype. For example, the assignment of geotypes on the basis of projected PSMB traffic profiles in different geographical areas would not meet this criterion, because no such dataset exists.

Second, the basis on which geotypes are defined must also yield classes whose members are sufficiently homogenous in terms of PSMB demand and supply characteristics. That is, any geographical area should ideally be more similar to areas with the same geotype than to areas of a different geotype. For example, the assignment of geotypes on the basis of rainfall levels would not meet this criterion, because there is no reason to believe that areas with similar rainfall would have similar PSMB requirements.

In view of this, geotypes have been specified on the basis of population density. This is based on the assumption that population density is a reasonably good indicator of:

- where assets (including lives and property) are physically located and hence where PSA activity is likely to be concentrated
- the type and frequency of incidents that are likely to occur.

As such, population density can provide an indication of the nature of demand for PSMB services and hence the type of network solutions that would need to be implemented in each area. A similar approach has also been used in other studies (Analysys Mason 2015).

Accordingly, five geotypes based on population density have been specified (table C.1). These threshold definitions have been adopted from ACMA (2014b) with some modifications. Specifically, while ACMA (2014b) distinguished between metropolitan and regional areas in the urban and suburban geotypes, this study does not.

Table C.1 **Geotype definitions**

Geotype	*Resident population density (persons/km^2)*
Dense urban	3 000+
Urban	1 250 - 3 000
Suburban	100 - 1 250
Rural	0.2 - 100
Remote	less than 0.2

Source: Adapted from ACMA (2014).

What statistical data are used?

Once the decision has been made to use the geotype definitions (table C.1), there is still the question of what statistical data are used to categorise and aggregate geographical areas into geotypes. The ABS reports population data at a number of different levels of aggregation ('spatial units'), meaning various levels of geographic granularity could be used (box C.1).

Box C.1 Spatial units in the Australian Statistical Geography Standard

The ABS publishes geographic statistics using a common hierarchical classification system of geographical regions called the Australian Statistical Geography Standard (ASGS). Under this Standard, geographical areas are classified within the following taxonomic ranks ('spatial units').

Spatial unit	*Count*	*Smallest Block (km^2)*	*Largest Block (km^2)*
Mesh Block	347 627	0.0001	165 217.0
Statistical Area Level 1 (SA1)	54 805	0.002	328 721.5
Statistical Area Level 2 (SA2)	2 214	0.8	519 519.0
Statistical Area Level 3 (SA3)	351	10.6	714 833.2
Statistical Area Level 4 (SA4)	106	57.6	2 298 053.2
Greater Capital City Statistical Areas	34	217.7	2 520 156.3
State and Territory	9	217.7	2 526 574.2

For each of these spatial units, the ABS reports on the size (in km^2) of each block as well as the Usual Resident Population based on 2011 census data. For SA2 spatial units and larger, the ABS also reports Estimated Resident Population on an annual basis.

Sources: ABS (*Australian Statistical Geography Standard (ASGS): Volume 1 - Main Structure and Greater Capital City Statistical Areas*, July 2011, Cat. no. 1270.0.55.001; *Socio-economic Indexes for Areas (SEIFA), Data Cube only, 2011*, Cat. no. 2033.0.55.001).

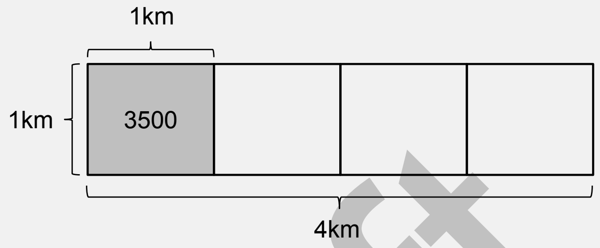
The choice of spatial unit has significant implications, as there are tradeoffs associated with the level of granularity used.

On the one hand, the choice of a spatial unit with larger boundaries runs the risk of aggregating very dissimilar areas into the same block. Areas within the same block are treated as though they were homogenous, whereas in practice populations tend to be clustered in towns and cities. This could lead to excessive 'averaging' of population density, which would misrepresent the geographic distribution of Australia's population. An example of this is discussed in box C.2.

On the other hand, a spatial unit with boundaries that are too small will not accurately reflect the geographic scale at which networks are designed. This could cause excessive fragmentation of geotype areas for the purpose of network dimensioning. Specifically, if the coverage of a network cell is larger than the size of a statistical block, there may be inaccuracies in the calculation of how many cells are required. An example of this is discussed in box C.3.

Box C.2 Large blocks lead to 'averaging' of population density

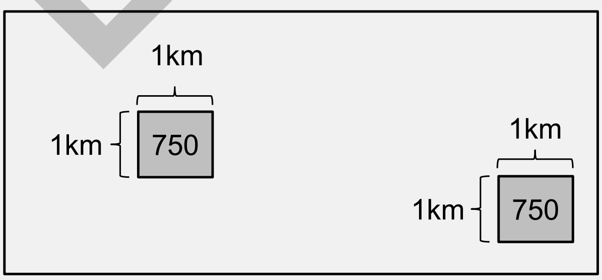
Consider four small geographical blocks, each with dimensions of 1 km x 1 km (illustrated below). Suppose one of these blocks (say, a town) has a residential population of 3000 and the other three have a residential population of zero. At this level of aggregation, the first block would be assigned a dense urban geotype, and the remainder would be classified as remote.



However, suppose these four areas were aggregated into one large block. Now, the larger block would be assigned a suburban geotype. For the purpose of network dimensioning (discussed later), this carries the implicit assumption that the residential population is uniformly distributed across all four smaller blocks; as a result, the network would need to provide coverage to all four blocks (which is not the case).

Box C.3 Small blocks lead to fragmented geotype areas

Consider two small geographical blocks (illustrated below), each with dimensions of 1 km x 1 km, a residential population of 750 and hence a suburban geotype. The surrounding areas are uninhabited, with a residential population of zero.



For the purposes of network dimensioning, the two blocks would be combined to obtain the total coverage area for the suburban geotype class (section C.4). As a result, coverage for this geotype class is determined as though its areas were contiguous.

However, if a network cell has an effective site area sufficiently larger than a single block (say, 2 km^2), the number of cells required will be underestimated. In this case, the network dimensioning approach would report that one cell (of 2 km^2) is required to provide coverage to the two blocks (of 1 km^2 each), whereas in practice, because the blocks are nonadjacent to each other, two cells would be required.

Bearing these considerations in mind, the decision was made to use data reported by the ABS at the SA2 level. This was chosen with a view to minimising the size of blocks, subject to the smallest block being no smaller than the coverage area of a single cell (sections C.5 and C.6). (Data reported at the SA1 level were deemed to be too granular, with the smallest SA1 block being 0.002 km^2 in area, compared with 0.8 km^2 for the smallest SA2 block.)

For each block, population density is calculated by dividing estimated residential population (as at 2014) by the total area of the block. Each block is assigned a geotype on the basis of population density. Table C.2 summarises how the area and population of Australia is distributed between each geotype class.

Table C.2 **Area and population within geotypes**

Geotype	*Density*	*Population*	*Area*	*Average population density*	*Percentage of total population*	*Percentage of total area*
	pop/km^2	millions	km^2	pop/km^2	%	%
Dense urban	>3 000	3.07	740	4 146	13.75	0.01
Urban	1 250 – 3 000	7.83	4 067	1 924	35.05	0.05
Suburban	100 – 1 250	7.42	22 130	335	33.22	0.29
Rural	0.2 – 100	3.78	1 423 207	2.7	16.95	21.03
Remote	<0.2	0.23	6 237 665	0.04	1.03	78.62
All		22.32	7 687 809	2.9	100.00	100.00

Sources: ABS (*Australian Statistical Geography Standard (ASGS): Volume 1 - Main Structure and Greater Capital City Statistical Areas*, July 2011, Cat. no. 1270.0.55.001; *ABS.Stat - ERP by SA2 (ASGS 2011), 1991 to 2014*).

C.4 RAN dimensioning

A radio access network consists of typically thousands of sites (or 'cells'), both logical and physical (box C.4). The number of sites required over time for a PSMB network has implications for the volume of inputs (such as site equipment and site upgrades) required and hence the total cost of delivering a PSMB capability.

Box C.4 Logical and physical sites

Some of the literature on mobile networks differentiates between logical and physical sites. For example, Analysys Mason (2015, pp. 2–3) stated that:

> … [t]he total number of logical sites [refers to] the total number of 2G sites plus the total number of 3G sites plus the total number of 4G sites. It should be noted that the total number of logical sites is considerably higher than the total number of physical sites in Australia, because it is quite common for the operators to co-locate more than one technology on a single physical site; and in some cases a single physical site may also be shared by more than one operator.

A 'site' used for delivering a PSMB capability generally refers to a particular logical site and the physical site on which it is located. Ordinarily, these physical sites are shared with other communications service providers, such as mobile carriers or land mobile radio networks. A special case is a 'greenfields site build', which implies a new physical as well as a new logical site.

Source: Analysys Mason (2015).

As discussed in section C.3, a site-by-site approach to estimating the number of sites is considered too data intensive for the task at hand. Similarly, use of commercial networks as a benchmark would not be appropriate for all areas, as it would likely overestimate the number of sites required in more densely populated regions, since mobile carrier networks are designed to meet commercial traffic.

This section discusses how the number of RAN sites for the dedicated component of a network is estimated. The approach to RAN dimensioning stems from the broader geotyping framework that links geographical areas to PSMB demand and supply characteristics. For each year within the time horizon, it calculates the number of sites required for each geotype class in each state ('state–geotype class').

A two-pronged approach to estimating sites

The number of required sites is estimated using two different methods, depending on the geotype of the area to be covered.

Dense urban, urban and suburban areas

In dense urban, urban and suburban areas, the number of sites is calculated using a bottom-up approach (the ‘RAN dimensioning approach’). This involves calculating, for each state–geotype class, the number of sites necessary for coverage (‘coverage sites’) and the number of additional sites required to meet a specified level of traffic (‘capacity sites’). The RAN dimensioning approach is discussed in further detail later in this section.

Rural and remote areas

In general, larger SA2 blocks tend to have a lower population density, with the largest 20 per cent of blocks exclusively classified as regional or remote. In these areas, population is not uniformly distributed over the block area, but is typically concentrated in a small number of population centres. Additionally, these areas are more likely to include economic assets that are not tied to reported population centres, such as roads and rail lines. For these reasons, SA2 blocks as a whole would not be a good indicator of where PSA operations take place and hence where PSMB services would be required.

As a result, the required number of sites is estimated by reference to the number of physical 3G sites operated by mobile carriers in the 850 or 900 MHz band (table C.3). It is assumed that mobile carrier sites in these areas and bandwidth are coverage-dimensioned; therefore, 100 per cent of those sites would need to be used by a PSMB network in order to achieve the same level of coverage. (This will overstate the number of sites required if some of these sites are deployed for capacity rather than coverage purposes.)

Table C.3 **Number of unique mobile carrier 3G sites**
For rural and remote areas

	Rural			*Remote*		
	Telstra[a]	*Optus*[b]	*VHA*[c]	*Telstra*[a]	*Optus*[b]	*VHA*[c]
NSW	697	704	313	72	29	16
Vic	579	529	212	31	27	10
Qld	553	461	200	176	66	16
SA	257	202	115	70	27	15
WA	280	186	119	308	45	17
Tas	137	80	29	0	0	2
NT	45	24	9	55	6	6
ACT	16	21	13	1	4	2
Total	2 564	2 207	1 010	713	204	84

[a] 850 MHz band. [b] 900 MHz band. [c] 850 and 900 MHz bands.

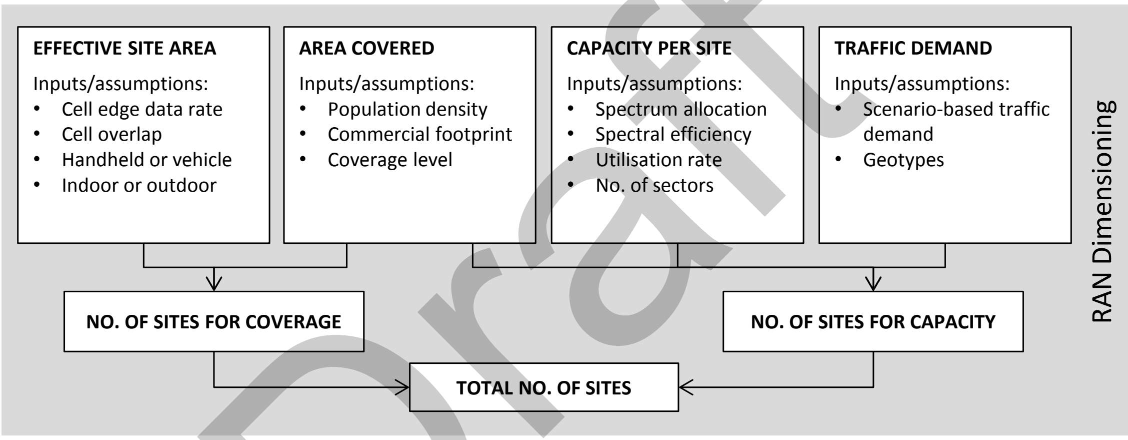
Sources: Productivity Commission estimates based on ACMA (2015e); ABS (*Australian Statistical Geography Standard (ASGS): Volume 1 – Main Structure and Greater Capital City Statistical Areas*, July 2011, Cat. no. 1270.0.55.001; *ABS.Stat – ERP by SA2 (ASGS 2011), 1991 to 2014*).

Overview of the RAN dimensioning approach

The RAN dimensioning approach is a bottom-up approach for estimating the number of sites required to service a specified coverage area. It does so by calculating the number of coverage and capacity sites in each state–geotype class within the coverage area (figure C.2).

For each state–geotype class, the total number of sites required is the maximum of the number of coverage sites and the number of capacity sites. In practical terms, this is equivalent to rolling out the required number of coverage sites, with additional capacity sites targeted to meet high-traffic areas where necessary.

Figure C.2 **Overview of the RAN dimensioning approach**



RAN dimensioning approach: coverage sites

For each state–geotype class, the RAN dimensioning approach calculates the number of coverage sites required. The number of coverage sites is given by the total area to be covered, divided by the effective area of each site ('effective site area'), rounded up. That is, for each geotype (G) in each state (S):

$$coverage\ sites_{G,S} = \left\lceil \frac{total\ coverage\ area_{G,S}}{effective\ site\ area_{G,S}} \right\rceil$$

It is assumed that the number of sites required to provide coverage to these areas will not change over time.

Total coverage area

The coverage area for each state–geotype class is calculated using ABS data relating to the geographic size of SA2 divisions. Table C.4 summarises the total geographic area in each geotype for each state and territory.

Table C.4 **Geographic area of geotypes**
By state and territory

State	*Dense Urban*	*Urban*	*Suburban*	*Rural*[a]	*Remote*[a]	*Total*[b]
	km^2	km^2	km^2	km^2	km^2	km^2
NSW	523.7	906.4	6 916.2	482 206.9	310 255.6	800 808.8
Vic	234.2	1 059.6	5 679.5	193 337.3	27 185.1	227 495.7
Qld	75.2	870.9	4 889.3	336 757.1	1 387 365.6	1 729 958.1
WA	-	442.5	1 485.9	138 039.1	844 211.8	984 179.3
SA	27.2	623.2	2 494.4	174 543.0	2 348 886.3	2 526 574.2
Tas	-	42.6	878.7	54 004.8	13 092.1	68 018.2
NT	1.5	38.8	133.6	53 986.8	1 294 038.0	1 348 198.7
ACT	1.4	181.9	88.3	918.9	1 167.4	2 357.9
Other	-	-	-	217.7	-	217.7
Total[a]	863.2	4 166.0	22 565.9	1 434 011.6	6 226 202.0	7 687 808.6

[a] The RAN dimensioning approach is not applied to these geotypes. [b] May not sum due to rounding.
Source: ABS (*Australian Statistical Geography Standard (ASGS): Volume 1*, Cat. no. 1270.0.55.001).

Effective site area

For each geotype (G), the effective site area (ESA) is calculated using the following equation:

$$ESA_G = \pi \times (r_G)^2 \times (1 - CO)$$

where r_G is the cell range (or 'maximum cell radius') for that geotype and CO is a factor describing how cells overlap with each other. A greater CO indicates greater cell overlap and lower unique coverage.

Estimating the maximum cell radius requires an understanding of the factors that influence it. This involves using:

- a link budget to estimate the maximum allowable propagation loss (MAPL) – which is a metric of how much signal degradation can be tolerated
- a propagation model, with various embedded assumptions, to translate an MAPL estimate into a maximum cell radius.

A link budget is an engineering tool which — accounting for all the expected gains and losses — calculates the maximum path loss between the transmitter and the receiver. From a technical perspective, link budgets can involve many different inputs and assumptions, including (ECC 2013):

- the maximum base station transmission power
- the signal to noise ratio
- the type of receiver (handheld or vehicle device), which affects 'body loss'
- whether the receiver is indoors or outdoors (since buildings contribute to signal losses)
- minimum cell edge data rate (since a higher data rate requires a stronger signal).

Propagation models are used to estimate a relationship between signal losses and distance from the antenna. The maximum cell radius is taken to be the distance at which signal losses are equal to the MAPL. There are various propagation models, with different inputs and assumptions, including assumptions about antenna height. The choice of propagation model — along with assumptions about the height of a base station antenna — can have a material effect on estimated cell ranges.

Calibration of cell radius for each geotype is discussed further in section C.6.

RAN dimensioning approach: capacity sites

For each state–geotype class, the number of capacity sites (for both downlink and uplink traffic) is calculated as the volume of total traffic, divided by the capacity of each site, rounded up. That is, for each geotype (G) in each state (S):

$$capacity\ sites_{G,S} = \left\lceil \frac{total\ traffic_{G,S}}{site\ capacity} \right\rceil$$

The number of capacity sites will grow from year to year, in line with growth in traffic.

Traffic scenarios

For each geotype (G), uplink and downlink traffic per square kilometre (in Mbps/km^2) for each year (t) is described by the following equation:

$$traffic_{G,t} = TPD_{G,t} \times ND_G \times P$$

where:

- $TPD_{G,t}$ is throughput per device (uplink or downlink), for a given year and geotype. It is assumed to grow from year to year at a constant growth rate
- ND_G is the number of devices per square kilometre for each geotype

- P is the proportion of devices that are online at a given point in time, relative to the total number of devices in that area.

These values are calibrated with reference to traffic scenarios, as discussed in chapter 4. Total traffic for each state–geotype class is calculated for each year by multiplying traffic per square kilometre by the total area in each state–geotype class.

Site capacity

For uplink and downlink, the capacity per site (SC) in year t is calculated using the following equation:

$$SC = S \times SA \times SE_t \times U$$

where:

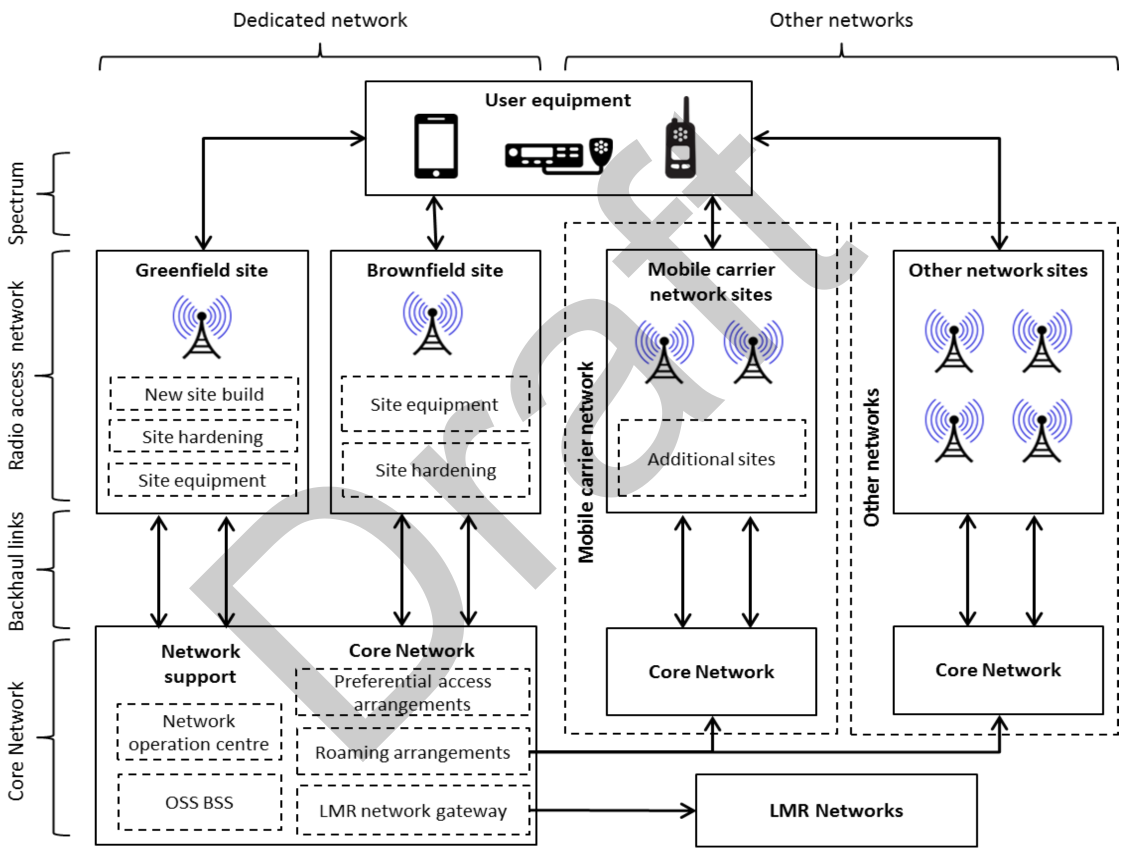
- S is the number of sectors per site. In the dense urban, urban and suburban geotypes, it is assumed that each site has three sectors ($S = 3$)
- SA is the spectrum allocation to be used in MHz. For options involving a dedicated network, this is the quantum of dedicated spectrum. For commercial approaches, this value is set sufficiently high so that the number of capacity sites is non-binding. This means that, for commercial approaches, only the number of sites required for coverage will be hardened, and PSA capacity requirements in excess of this will be met by other commercial network sites
- SE_t represents spectral efficiency in bits per second per Hertz (bits/s/Hz) in year t. This is a measure of how much information can be carried by a particular amount of spectrum and depends on the development of technology over time. It is influenced by two key factors: the types of antennae deployed and the capabilities of the end-user devices on the networks. Spectral efficiency typically increases in steps with new versions of mobile technology (such as 3G to 4G standards) and improved antenna technology, though it can take time for base stations to be upgraded to the latest standards and there are technical limitations on how far it can continue to improve (Analysys Mason 2015)
- U is the maximum cell loading factor, which is a measure of how much a network can be practically loaded before users experience material issues with quality of service. High cell loading can lead to congestion and materially slow down data transmission.

The calibration of these values is discussed further later in this appendix (section C.6).

C.5 Network costing

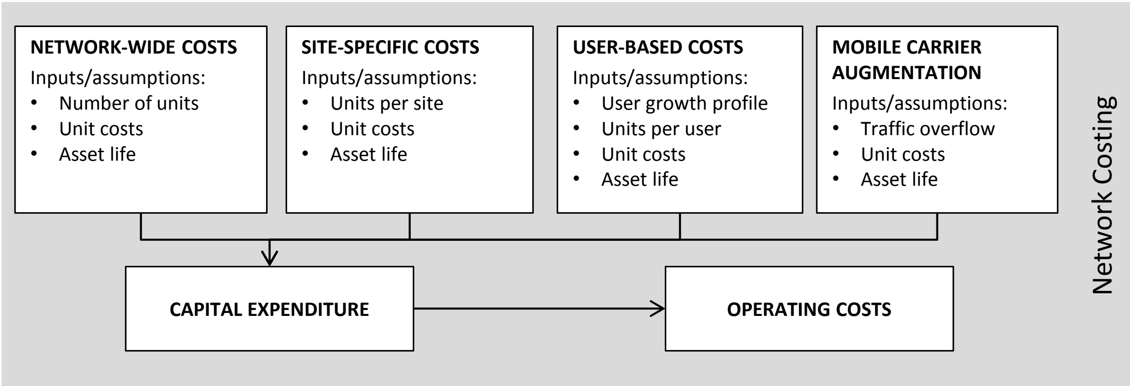
Communications networks are comprised of many different component parts. Figure C.3 gives a stylised representation of how information is transmitted across a mobile broadband network and highlights some of the key infrastructure, equipment and technologies that would be required to deliver a PSMB capability.

Figure C.3 **Stylised PSMB network**



The network costing module of the quantitative analysis estimates the capital expenditure and operating costs of delivering a PSMB capability under different options. A bottom-up costing approach is taken, whereby the total cost is estimated by aggregating individual component costs. An overview of the approach to network costing is depicted in figure C.4.

Figure C.4 **Overview of network costing approach**



Approach to estimating capital expenditure

The value of capital expenditure items ($CAPEX$) is calculated as the product of discounted unit costs and the number of additional units required in each time period, summed across all items and over time:

$$CAPEX = \sum_{j=1}^{N}\sum_{i=1}^{T} \delta_i \times unit.cost_j \times no.units_{i,j}$$

where δ_i is the discount factor, for all cost items in $\mathrm{N} = \{1, 2, \dots N\}$ and all years within the time horizon $\mathrm{T} = \{1, 2, \dots T\}$.

The unit cost of each capital expenditure item is specified exogenously. Calibration of unit costs is discussed further in section C.6.

For each item, the total number of units required over the time horizon is derived in one of four ways.

1. For some cost items, the total number of units required is specified *exogenously*.
2. In cases where the total number of units required is *site dependent*, the number of units is expressed as a proportion of RAN sites.
3. For some cost items, the number of units required is *user dependent*. This includes end-user devices and augmentation of mobile carriers' core networks to account for increases in traffic.
4. Some capital expenditure arises from the *augmentation* of existing mobile carrier RAN infrastructure. For delivery options involving overflow of PSA traffic onto commercial networks, this includes any upgrades to those networks necessary to meet increased traffic volumes.

For each of these items, the number of additional units required each year is also affected by rollout times and the length of asset lives (discussed below).

Table C.5 summarises capital expenditure items and how they are captured and represented in the quantitative analysis.

Table C.5 **Capital expenditure items**

Cost item	*Variable name(s)*	*Type*	*Description*
Radio access network			
New deployment	NewSiteBuildMetro	site-dependent	Greenfields site in dense urban, urban or suburban area
	NewSiteBuildRegional	site-dependent	Greenfields site in rural or remote area
Site equipment	SiteEquipment	site-dependant	Deployment of new site equipment
Site hardening costs			
Power backup	Battery20	site-dependant	Additional 20 hours of power backup
	Battery24	site-dependent	24 hours of power backup
Civil site upgrade	Civil	site-dependant	Civil and security upgrades to a site
Core network and add-ons			
New deployment	CoreNational	exogenous	Deployment of new national core network (including redundant core)
	CoreState	exogenous	Deployment of new state core network (including redundant core)
Preferential access	PreferentialAccess	exogenous	Upgrades to a core network to allow preferential access
LMR network gateway	LMRIntegration	exogenous	Upgrades to core network to link to LMR networks
OSS, BSS	OSSBSS	exogenous	Operation and billing support systems and other network management
User equipment			
End-user devices	Handset	user-dependent	Off-the-shelf mobile device
	RuggedisedHandset		Ruggedised mobile device
	IVModem		In-vehicle device
Spectrum			
Dedicated spectrum	Spectrum	exogenous	Spectrum to support dedicated network
Mobile carrier network augmentation			
New sites	MNOSitesAugmentation	augmentation	Additional mobile carrier sites required to meet PSA traffic
Core network augmentation	CoreNetworkAugmentation	user-dependent	Mobile carrier core network augmentation required to meet PSA traffic

Exogenous items

The number of units required for some items is determined exogenously, generally as part of option design (chapter 6).

- For all options involving a dedicated network, the quantum of dedicated spectrum is specified as part of option design.
- Whether the network is implemented at a national level or on a state-by state basis has implications for the number of core network items required. Where a new core network is deployed, it is assumed that a new operations and business support systems and network operations centre would also be required to manage and operate the network.
- The number of mobile carriers involved in delivering the dedicated network has implications for the extent of LMR integration required.

Site-dependent items

For some items, the total number of units required depends on and is expressed as a proportion of the number of RAN sites. These items fall into two broad categories: items relating to site builds and site hardening.

Radio access network

It is assumed that the deployment of the dedicated component of the network is comprised of a mix of brownfield and greenfield site builds. For the proportion of sites requiring a greenfield build, a new site build cost is applied.

It is also assumed that new site equipment is required at all RAN sites, regardless of whether the build is greenfield or brownfield. This is because it is assumed that the use of dedicated spectrum (which underpins the dedicated network) is not supported by equipment that is currently installed at RAN sites. That said, the extent of new equipment required, and whether some equipment can be shared, is tested through sensitivity analysis (section C.8).

Hardening

To meet PSA reliability requirements, it is assumed that a proportion of sites are subject to some form of network hardening. For the purposes of quantitative evaluation, hardening is assumed to involve three categories of capital investment:

- installation of additional battery backup at some proportion of mobile sites (beyond the capabilities already deployed at mobile carrier sites)

- civil works to increase the physical resilience of some proportion of mobile sites to protect against failures caused by high winds, fire and floods (such as by strengthening masts), and measures to improve site security
- deployment of new backhaul links at some proportion of mobile sites without geographically diverse backhaul (to ensure redundancy of transmission).

Of these, additional battery back-up and civil upgrades are treated as site-dependent items. The cost of deploying new backhaul links is captured as part of backhaul operating costs (discussed later).

User-dependent items

The number of units required of some items is expressed as a proportion of PSA users from year to year. For each geotype (G) in each state (S), the number of users in year t is determined as:

$$No.users_{G,S,t} = N_{G,S} \times \left(1 + R_{G,S}\right)^{t-1}$$

where $N_{G,S}$ is the number of users in year 1 and $R_{G,S}$ is the rate of growth from year to year.

Two types of capital expenditure items are treated as being user-dependent: end-user devices and core network augmentation.

End-user devices

The number of end-user devices required is causally dependent on the number of PSA users. This includes standard handsets, ruggedised handsets and in-vehicle modems.

Core network augmentation

For options involving a mobile carrier network, total capital expenditure also includes any upgrades of the mobile carrier core network required to meet additional PSA traffic (as preferential users). The magnitude of core augmentation required from year to year is also estimated with reference to the number of devices. In practice, the core network is augmented to account for increases in the volume of traffic over time. However, given the lack of robust traffic forecasts for a PSMB capability, the Commission's analysis uses the number of PSA users as a proxy for total traffic volumes.

Augmentation of mobile carrier networks

For options involving a commercial mobile carrier network, total capital expenditure inludes any incremental investments made to the network in order to meet additional demand that derives from PSA traffic over the evaluation period ('overflow traffic').

This is based on the premise that while adding PSA traffic to an existing commercial mobile network may not lead to the same requirement for upfront capital expenditure as in a dedicated option, it is not costless. In particular, any additional traffic can be expected to have an effect on forward looking capital and operational decisions by mobile carriers. The extent of this impact will depend on a range of factors, including:

- the amount of PSA traffic
- the timing and duration of PSA traffic loads
- the manner in which PSA traffic interacts with existing traffic on commercial networks, which have been dimensioned to accommodate some measure of 'busy hour' demand at each cell site.

Table C.6 summarises how PSA traffic is carried across the dedicated and mobile carrier network under the different options specified in this study.

Table C.6 **How PSA traffic is carried under different options**

Approach	*Dedicated network*	*Mobile carrier network*
Dedicated	All PSA traffic	..
Commercial	..	All PSA traffic
Hybrid, geographical areas with dedicated network	Some PSA traffic	Some PSA traffic (overflow traffic)
Hybrid, geographical areas without dedicated network	..	All PSA traffic

.. Not applicable

Characterising overflow traffic

As discussed in chapter 4, the Commission has adopted a scenario-based approach to characterising the level of capacity delivered by a PSMB capability. Accordingly, the total network is dimensioned to meet the level of capacity arising from certain scenarios.

For options involving a mobile carrier network component, the volume of overflow traffic is expressed as a proportion of total traffic — that is, for each geotype (G) in each state (S):

$$overflow\ traffic_{G,S} = \omega_G \times total\ traffic_{G,S}$$

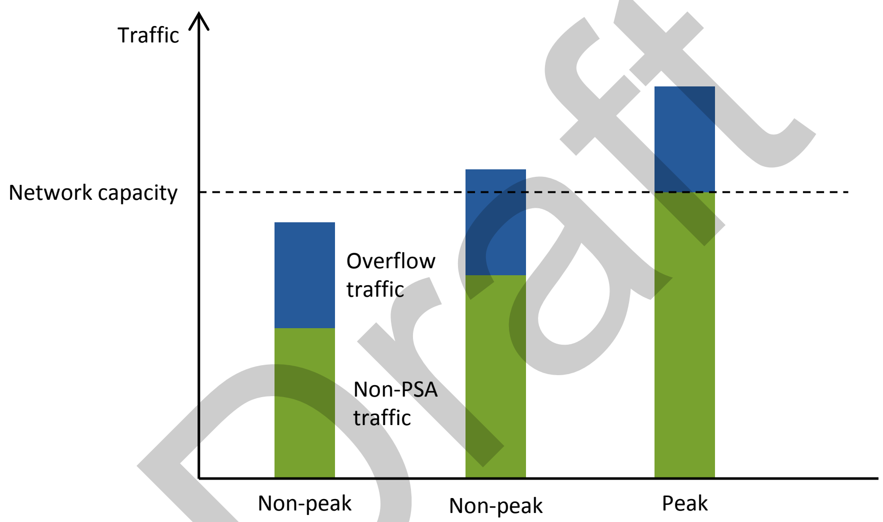
where ω_G is a constant that describes the proportionate relationship.

Overflow traffic and excess capacity on the mobile carrier network

The effect of overflow traffic on the mobile carrier network at any given instance will depend on how much excess capacity is in that network at the time. The degree of congestion on a network depends on total traffic volumes, so overflow traffic is less likely to cause congestion when commercial traffic is low than when commercial traffic is high.

Figure C.5 depicts how the same volume of overflow traffic could have different implications for a mobile carrier's network, depending on the level of non-PSA traffic and whether PSA overflow demand coincides with commercial peak periods.

Figure C.5 **Overflow traffic and excess capacity**



For dense urban, urban and suburban areas, this analysis is agnostic about *when* PSA overflow occurs — specifically, this means that overflow traffic could coincide with commercial peak usage and hence mobile carriers will need to dimension their networks to meet traffic in such an eventuality. It is also assumed that, during the commercial busy hour peak, mobile carriers have zero excess capacity that can be leveraged to meet overflow traffic. This assumption could lead to an overestimate of the cost of capacity augmentation on carrier networks, on the basis that mobile carriers have:

- significant portfolios of spectrum to draw on
- heterogeneous networks made up of various technologies and diverse cell types
- access to technologies and alternative technologies to boost capacity in localised areas, such as carrier aggregation, Wi-Fi networks and deployable cells (chapter 5).

As discussed in section C.4, it is assumed that, for the duration of the evaluation period, the RAN in rural and remote areas is coverage dimensioned. Here, it is further assumed that, in these areas, there is sufficient excess capacity to meet any overflow traffic during the evaluation period, which will tend to underestimate costs in these areas. (In practice, additional traffic could also be met using alternative or supplementary technologies, which are not included in the quantitative analysis.) To capture this, the level of overflow traffic in these areas is set to $\omega_G = 0$, which is equivalent to setting $additional\ sites_{G,S} = 0$ in these geotypes.

Estimating mobile carrier response to overflow traffic

In general, mobile carriers can provision for additional traffic in one of three ways:

1. building additional sites to increase capacity in targeted areas
2. purchasing additional spectrum to allow existing sites to carry more traffic
3. using existing capacity, but possibly lowering the quality of service provided to other customers.

In the absence of detailed information about each mobile carrier's network architecture at a site-by-site level, the likely pattern and intensity of PSA demand across mobile sites or in different areas, as well as accurate information about the relative cost of different approaches, it is impossible for the Commission to predict how, in practice, network augmentation would be implemented.

For the purpose of quantitative analysis, the cost of capacity augmentation is estimated by evaluating the number of new sites that would be needed to carry overflow traffic. Specifically, for each geotype (G) in each state (S), the number of additional sites is calculated by dividing total overflow traffic by the capacity of a single site:

$$additional\ sites_{G,S} = \frac{overflow\ traffic_{G,S}}{site\ capacity}$$

This is based on the assumptions that:

- there is no change in mobile carrier spectrum holdings
- there is no degradation of service quality to other customers.

In other words, it is assumed that additional traffic on mobile carrier networks is met exclusively through additional site builds. It is expected that these assumptions will overestimate the cost of mobile carrier capacity augmentation, as they discount the fact that the same level of augmentation could be achieved on a mobile carrier's network at less cost using a different mix of inputs (that is, a mix of additional spectrum, additional sites and existing capacity, or use of alternative technologies).

This approach also assumes that overflow traffic is spread across the network in a particular way, bearing in mind the fact that sites are not divisible over different geographical areas. That is, an additional site can only provide additional capacity to areas within its cell radius, whereas in practice overflow traffic might be spread over a wider geographical area. However, because capacity augmentation to meet overflow traffic would likely take place as part of a mobile carrier's broader investment plans to meet increased demand generally, additional sites can be shared between PSAs and other users. In that sense, additional sites for overflow traffic is used a proxy for the costs that would be attributed to PSAs.

Effect of additional sites on the use of existing spectrum holdings

To support the use of additional sites, mobile carriers would need to use some of their existing spectrum holdings to make these sites operational. The opportunity cost of doing so should be assessed with reference to the extent to which that spectrum's present and future use is encumbered by its use at these additional sites.

In sparsely or moderately populated areas, where sites are widely spaced, it is likely that additional sites will have zero effect on the use of spectrum by other sites, whether existing or future. However, in areas with high site density, it is possible that additional sites could negatively impact the efficiency of how spectrum is used at nearby sites.

This opportunity cost has not been quantified as part of the analysis. However, given that additional sites have no or marginal impact on the use of the same spectrum by existing sites, it is expected that this opportunity cost will be small.

Other possible approaches

The Commission has identified two alternative approaches to estimating the cost of mobile carrier network augmentation to meet overflow traffic.

The first approach involves using Analysys Mason's mobile network forecasting model, which was prepared for ACMA (Analysys Mason 2015). This model was designed to estimate the tradeoffs between spectrum and network infrastructure in meeting additional capacity requirements. At present, a version of this model that uses placeholder values for some variables is publicly available. However, because many key variables have been redacted and others are measured differently to the Commission's analysis (for example, in the Analysys Mason model, traffic demand is in the form of an annual volume whereas the Commission's analysis determines network capacity using traffic per second per square kilometre), use of this model has significant additional informational requirements.

Alternatively, mobile carriers' historical and forecasted capital expenditure could be used as an indication of the cost of increasing capacity over time. Accordingly, the growth in mobile carriers' subscriber bases could be considered analogous to adding PSA overflow traffic to the network (although services delivered to PSAs would require higher quality of service levels). An example of this is given in box C.5.

Box C.5 **Use of capital expenditure data to estimate augmentation costs**

Historical and prospective capital expenditure data could be used to estimate how increases in carriers' subscriber bases are matched by incremental investments.

By way of illustration, Telstra recently announced that over three years to June 2017 it expects to have invested more than $5 billion into its 4G mobile network. In its 2014 annual report, it reported that total retail mobile subscribers grew from 12.2 million to 16.0 million in the three years between 2011 and 2014. Assuming that Telstra would experience a similar growth in its user base in the three years to June 2017, the average capital expenditure per user (and hence the average additional cost per user) is approximately $1351.

Source: Telstra (2014b).

However, this approach faces several difficulties, including:

- the availability of sufficient data points
- the fact that historical data would include coverage (as distinct from capacity) investments and other investments which are 'fixed costs'
- the difficulty of mapping capacity investment costs to a corresponding increase in network capacity, given the limited information available.

INFORMATION REQUEST

What types of costs arise from augmenting mobile carrier networks to meet PSA traffic? What is the appropriate approach to estimate these costs? Are there alternative methods that could be used as robustness checks?

Timing of capital expenditure

The present value of capital expenditures is also affected by when costs are incurred. This includes considerations of when assets are rolled out, how frequently they are replaced and the timeframe captured by the evaluation period.

Rollout schedule

For each capital expenditure item, a schedule of how long it takes to roll out the asset is specified. In general, items that are essential to the operation of the network as a whole (such as the core network) are assumed to have a rollout period of one year. Items that are more 'scalable' (such as handsets and site equipment) are generally assumed to have longer rollout periods.

For simplicity, it is assumed that investment costs are incurred at the same time as an asset is rolled out. It is also assumed that assets are rolled out uniformly over the rollout period; for example, if handsets have a rollout period of five years, it is assumed that 20 per cent of the total number of handsets would be rolled out in each of those years.

Asset life span and replacement

The asset life span for each capital expenditure item is also specified, which defines how often an asset must be replaced. It is assumed that, when the asset is replaced, the replacement schedule is identical to the rollout schedule.

If the replacement schedule extends beyond the time horizon of the quantitative analysis, only capital expenditures made within the time horizon are counted. Furthermore, at the end of the time horizon, the asset will be deemed to have been partially replaced, in accordance with the proportion of the replacement schedule that falls within the time horizon.

For example, suppose the replacement of site equipment takes five years and begins in year 17. If the time horizon for the analysis is 20 years, only the investments made in years 17-20 (that is, four years) will be counted and at the end of the time horizon the asset will be deemed to have been 80 per cent replaced.

Residual value of assets

Some capital expenditures have an economic life that extends beyond the time horizon of the quantitative analysis. In such cases it is inappropriate to attribute all of the investment cost to the time horizon being analysed. In particular, investments made in the later years of the time horizon will be used for fewer years than the length of their economic life.

As a result, correction needs to be made for the proportion of the investment that operates outside of the time horizon. Accordingly, capital costs are truncated by first calculating the residual value of the asset at the end of the time horizon, assuming linear depreciation of the asset. The residual value is then applied as a negative capital expenditure at the end of the time horizon.

For example, suppose site equipment is replaced in year 17 and has a life span of eight years. If the time horizon for the analysis is 20 years, the residual value of the asset is calculated for the duration of its life span outside the time horizon (that is, years 21-24).

Operating costs

Based on approaches to calculating operating expenses in other studies (Brinkmann et al. 2007; Ofcom 2006) and feedback from study participants, three categories of operating costs have been identified:

- direct network operating costs
- network support operating costs
- common organisational-level costs.

The manner in which direct network and network support operating costs are estimated is discussed below. Common organisational-level costs have not been quantified as part of the analysis (section C.9).

Direct network operating costs

Direct network operating costs include expenditures relating to the operation and maintenance of elements directly related to providing a Long Term Evolution (LTE) service capability, such as base station equipment and core network infrastructure.

It is common practice to estimate the annual operating costs of particular items using expense ratios (Brinkmann et al. 2007; Nokia Siemens Network 2010). Expense ratios describe how operating expenditures vary in proportion to the value of another expense, and implicitly define a production relationship between two outputs.

In the present analysis, direct network operating costs for each item are estimated as a proportion of initial capital costs on a per-unit basis. In other words, the total direct network operating cost is calculated as the product of year-one unit costs (discounted), the number of operational units and a scalar that describes the proportionate relationship between operating and capital costs (α_j), summed across all items and over time:

$$OPEX.DN = \sum_{j=1}^{N}\sum_{i=1}^{T} \alpha_j \times \delta_i \times unit.cost_{1,j} \times no.units_{i,j}$$

where δ_i is the discount factor, for all cost items in $\mathrm{N} = \{1, 2, \ldots N\}$ and all years within the time horizon $\mathrm{T} = \{1, 2, \ldots T\}$.

This treatment of direct network operating costs assumes a linear relationship between direct network operating costs and initial capital costs, which also implies that:

- there are no scale efficiencies in operation and maintenance
- the composition of the network operator's assets is common across all options
- the tradeoff between capital investment and operating expenses is the same across all options.

Network support operating costs

Network support assets include annual site rental costs (for co-location at brownfield sites) and the annual purchase of all backhaul capacity from mobile sites back to the core network. These costs are estimated using per-unit market prices for site rental and backhaul capacity as a guide, on the assumption that these prices are the best publicly available estimates of underlying resource costs.

Specifically, the total network support operating cost is calculated as the product of discounted market prices and the number of operational units, summed across all items and over time:

$$OPEX.NS = \sum_{j=1}^{N} \sum_{i=1}^{T} \delta_i \times unit.cost_j \times no.units_{i,j}$$

where δ_i is the discount factor, for all cost items in $\mathrm{N} = \{1, 2, \ldots N\}$ and all years within the time horizon $\mathrm{T} = \{1, 2, \ldots T\}$.

Site leasing costs

The site leasing cost variable captures the opportunity cost of deploying new base station equipment at an existing site, as the use of space at a site precludes future use of that space for an alternative purpose. This opportunity cost is incurred regardless of who owns the site; in particular, for government-owned sites, the opportunity cost is the forgone value of alternative uses, such as leasing the space to another user.

However, under the commercial and hybrid approaches, it is assumed that mobile carriers use *existing* spaces. That is, mobile carriers replace their current site equipment with new site equipment in the same space. In these instances, there is no opportunity cost of deploying a new base station, as no additional space is being used.

Backhaul transmission networks

The backhaul transmission component of a mobile network comprises the links between the core network and each site (chapter 5). Broadly speaking, backhaul transmission is made up of three elements (ACCC 2014a):

- transmission between a group of mobile sites
- transmission from a point of aggregation to the core network (for example, from a town back to a capital city)
- transmission between one core network and other networks (for example, between capital cities).

Quantifying the costs of backhaul transmission networks is difficult because these networks are often complex in structure and topology. Various technologies are used for backhaul, including optical fibre, microwave and satellite, each with different technical properties, limitations and costs. Microwave is often cited as the dominant technology for transmission between sites and points of aggregation, with fibre more commonly used for trunk backhaul and in metropolitan areas. There is, however, significant variation between countries and mobile carriers (Ericsson 2013b).

Additionally, some elements of mobile backhaul transmission networks (particularly those responsible for carrying traffic to and from large numbers of sites) are designed in a 'ring', 'mesh' or 'tree' pattern to ensure there are multiple ways in which transmission traffic can be routed (ACCC 2014a; Ericsson 2014a; Nadiv and Naveh 2010). Other elements, such as links to individual mobile sites, may not have geographic diversity (Alcatel-Lucent, sub. 15; Optus, sub. 18).

Further, because mobile base stations do not always operate at maximum capacity, traffic from multiple sites will not be perfectly coincident. Accordingly, backhaul networks are typically dimensioned according to an 'overbooking factor', the level of which will depend on their position in the broader network. These techniques allow mobile carriers in particular (who aggregate and carry large volumes of traffic) to exploit the distribution of traffic across multiple sites.

In the absence of detailed information about the expected topology of a PSMB backhaul network, this analysis takes a simplified approach to estimating backhaul costs. Backhaul costs are estimated through a representative per-site cost that is intended to capture carriage of traffic between mobile sites to some point of aggregation (but not necessarily to the core network) and an annualised cost for new backhaul links to add greater geographic diversity to some proportion of sites (for hardening purposes).

For options involving commercial networks, it is assumed that the per-site backhaul cost is proportionately smaller. This assumption is made on the basis that:

- PSAs represent a very small proportion of the total customer base already served by mobile carriers
- mobile carriers already have (often high capacity) backhaul in place to their sites and may be able to add additional capacity at a lower per unit cost (there is some evidence available that the per-unit costs of adding backhaul fall as more is purchased (section C.6))
- mobile carriers are better able to optimise their broader network resources by using statistical multiplexing and differentiated classes of service to manage traffic loads within their backhaul/aggregation networks. In other words, meeting PSA traffic will not necessarily require significant additions to backhaul resources compared to the current capacity they utilise (Nadiv and Naveh 2010).

INFORMATION REQUEST

What is the appropriate approach to estimate the cost of backhaul? How are backhaul networks designed to meet levels of traffic? How does this differ between PSMB delivery options?

C.6 Calibration and inputs

This section discusses the key assumptions and estimated parameters used in the quantitative evaluation. In calibrating these assumptions and inputs, the Commission has reviewed a range of publicly available sources and studies (box C.6) and drawn on submissions from study participants. Feedback on certain technical matters on LTE networks was also sought from participants with relevant expertise in this area.

Box C.6 **Studies reviewed to inform inputs and assumptions**

Australian reports

- Analysys Mason (2015), *Mobile Network Infrastructure Forecasts.*
- Ernst and Young (2011), *Benefit Cost Analysis of National Broadband Capacity of Emergency Services Organisations.*
- Gibson Quai AAS Consulting (2011), *Public Safety Broadband Delivery Models (Project 2) for Public Safety Mobile Broadband Steering Committee, Final Report* (publicly redacted version).
- Access Economics (2010), *Radiofrequency Spectrum Options for Public Safety Agencies* (publicly redacted version).

International reports

- Alcatel-Lucent (2011), *High Level Total Cost of Ownership Comparison: Stand Alone Public Safety Network vs. Public Private Partnership,* Bell Labs.
- Federal Communications Commission (2010), *A Broadband Network Cost Model*, OBI Technical Paper No. 2.
- Nokia (2010), *Mobile Broadband with HSPA and LTE – Capacity and Cost Estimates.*
- Ericsson (2014), *Microwave Towards 2020 – Delivering High Capacity and Cost-Efficient Backhaul for Broadband Networks Today and in the Future*.
- ECC (2013), *User Requirements and Spectrum Needs for Future European Broadband PPDR Systems.*
- NPSTC (2012), *Priority and Quality of Service in the Nationwide Public Safety Broadband Network.*

General parameters and assumptions

Social discount rate

In accordance with the Office of Best Practice Regulation guidelines on cost–benefit analysis (OBPR 2014b), the Commission has used a central real discount rate of 7 per cent in calculating the net present value of each PSMB delivery option. As part of its sensitivity analysis, the Commission has also calculated net present values using real discount rates of 3 and 11 per cent (section C.8).

Time horizon

The Commission sought feedback from participants on the appropriate time horizon for the quantitative analysis. Two participants provided views:

- Telstra (sub. 19) proposed a 15-year time period based on the propensity for costs and benefits discounted over a longer periods of time to approach zero and the fact that spectrum licences in the 700 MHz band have a duration of 15 years.
- CDMPS et al. (sub. 7) suggested a horizon out to 2040 will take into account the release to market of 3GPP mission critical public safety communications standards-based products by 2020, and provide a 20-year period in which temporal changes in technologies and consumer demand can be reasonably assessed.

The quantitative evaluation in this study is based on a 20 year time horizon (2018–2037).

Network dimensioning: coverage

Coverage area

An underlying assumption for the quantitative evaluation is that all PSMB delivery options provide coverage to match the overall coverage footprint (99 per cent of the population) of mobile carriers nationally — but with different mixes of dedicated and commercial network elements depending on the option. Geotypes have been used as a basis for defining the coverage areas (table C.7).

- In options 1 and 2a – 2c, the dedicated PSMB network (supported by dedicated spectrum) covers 99 per cent of the population, which translates to 100 per cent coverage of dense urban, urban and suburban geotypes, and partial coverage of rural and remote geotypes.
- In options 3a – 3c, a dedicated PSMB capability (supported by dedicated spectrum) covers dense urban, urban and suburban areas only.
- In options 4a and 4b, commercial mobile carrier network coverage is used in all areas.

Table C.7 **Coverage of options by geotype category**

Option	*Dense urban*	*Urban*	*Suburban*	*Rural*[a]	*Remote*[a]
Option 1	Dedicated	Dedicated	Dedicated	Dedicated	Dedicated
Option 2	Dedicated and commercial	Dedicated and commercial	Dedicated and commercial	Dedicated and commercial	Dedicated and commercial
Option 3	Dedicated and commercial	Dedicated and commercial	Dedicated and commercial	Commercial	Commercial
Option 4	Commercial	Commercial	Commercial	Commercial	Commercial

[a] Coverage in these areas is provided using a number of sites equal to existing mobile carrier sites (that is, it roughly matches the coverage footprint of existing mobile carrier networks); as such, not all of the geographical area has coverage.

RAN dimensioning approach

A number of inputs used are required for the RAN dimensioning approach, including the geographic area of each state–geotype class, estimated max cell radii (based on various assumptions, such as antenna height and whether indoor or outdoor coverage is targeted), and an assumed cell overlap. Input on engineering matters was sought from a range of study participants.

The various assumptions relating to maximum cell radius and the central case estimates are set out in table C.8. Given that mobile carrier networks generally provide indoor coverage in dense urban, urban and suburban areas, it was assumed that a dedicated PSMB network would need to meet a commensurate standard of coverage.

Table C.8 **Assumptions used for maximum cell radius**

Indoor or outdoor	*Cell edge data rate*	*Dense urban*	*Urban*	*Suburban*
	kbps	km	km	km
Indoor	100	1.15	1.45	3.4
Indoor	256	0.875[a]	1.10[a]	2.6[a]
Indoor	750	0.6	0.75	1.8
Outdoor	100	2.5	3.14	7.4
Outdoor	256	1.75	2.20	5.2
Outdoor	750	1.25	1.57	3.7

[a] Central case estimate.

Benchmarking approach

For the benchmarking approach, publicly available data from the RadComms database (ACMA 2015e) were used to identify how many sites mobile carriers currently have, where they are located, how many are co-located, and what spectrum is deployed at each base station.

Because the intention was to identify the number of sites used to provide a coverage layer, only those sites using lower frequency spectrum were counted (based on the assumption that lower frequency spectrum is typically deployed for coverage purposes). Specifically, the mobile carrier site counts were based on sites deploying 850 and 900 MHz band spectrum.

The number of sites in each geotype was estimated by:

- creating a geotype map of Australia by importing SA2 shapefile data from the ABS into mapping software (QGIS), with geotypes assigned on the basis of population density
- overlaying the location of the sites used for coverage onto the geotype map

- a ‘points in polygon’ program was run, which counted the number of sites in each geotype (table C.3).

For each state–geotype class, the number of sites required for coverage is set equal to the maximum number of sites operated by any one carrier within that area.

Network dimensioning: capacity

Once a coverage layer is in place, additional sites are added when PSA traffic demand exceeds the capacity provided by the network. This is done so based on the average capacity of each site, which is derived using various assumptions and inputs (table C.9). A more detailed explanation of capacity dimensioning is presented in section C.4.

Table C.9 **Capacity dimensioning inputs**

Parameter	*Central case*
Average cell spectral efficiency	
downlink in 2018	1.6 bits/sec/Hz
uplink in 2018	0.79 bits/sec/Hz
downlink in 2037	3.37 bits/sec/Hz
uplink in 2037	1.66 bits/sec/Hz
Annual growth in spectral efficiency	4 per cent (per annum)
Maximum cell loading factor	75%
Number of cell sectors per site	
dense urban, urban and suburban geotypes	3
rural and remote geotypes	1

Spectrum allocation

For the purposes of the quantitative analysis in this study, it is assumed that spectrum in the 800 MHz band would be used for PSMB. This is consistent with ACMA’s previous proposition to allocate spectrum in this band for a PSMB capability, and efforts to harmonise spectrum in this band for the Asia-Pacific region. Two parcels of spectrum have been assumed for evaluation in the quantitative analysis — 2 x 5 MHz channels and 2 x 10 MHz channels (table C.10).

Table C.10 **Spectrum allocation**

Cost item	*Central case*	*Lower bound*	*Upper bound*
Spectrum	2 x 5 MHz	–	2 x 10 MHz

Importantly, these values are assumptions and do not amount to a finding or recommendation by the Commission that this spectrum should be used for delivering a dedicated PSMB capability. Ultimately, this is a matter for ACMA and the Minister for Communications and is beyond the scope of this report.

Traffic scenarios

As discussed earlier and in chapter 4, PSMB traffic has been characterised using a scenario-based approach. This is summarised in table C.11.

Table C.11 **PSMB traffic scenarios**

	Central case	*Lower bound*	*Upper bound*
Dense urban, urban and suburban			
PSMB traffic demand	1.5 Mbps/km^2	1 Mbps/km^2	4 Mbps/km^2
Growth rate	5% pa	2% pa	10% pa
Rural and remote			
PSMB traffic demand	500 Kbps/km^2	200 Kbps/km^2	800 Kbps/km^2
Growth rate	5% pa	2% pa	10% pa

Capital expenditure: number of units

This section discusses how the number of units for certain selected capital expenditure items has been derived.

Radio access network

When there is a dedicated network, new LTE base station equipment would need to be deployed to the number of sites required for coverage and capacity. In particular, it is assumed that new site equipment would be deployed in the central case.

In practice, existing mobile sites would be leveraged to the greatest extent possible to lower the costs of deploying site equipment. However, it is unrealistic to assume that all mobile carrier sites would have sufficient capacity to accommodate a new site equipment — especially where the dedicated network is not being integrated with a carrier's network. For this reason, it has been assumed that some of the sites required for a dedicated network would involve a greenfields build.

As a starting point, it has been assumed that 5 per cent of sites would be newly constructed, with a range from 0 to 15 per cent evaluated as part of sensitivity testing.

Table C.12 Proportion of new versus existing sites
Dedicated network

	Central case	*Lower bound*	*Upper bound*
Per cent using existing site	95%	100%	85%
Per cent requiring new site	5%	0%	15%

Hardening

As discussed earlier, it is assumed that hardening is required at a proportion of all sites. For commercial options, only those sites required for coverage will be candidates for hardening. For sites within a commercial network, it is assumed that fewer hours of additional battery backup are required at each site, as these sites would likely already have some level of battery backup. Table C.13 summarises the hardening parameters.

Table C.13 Assumed hardening parameters
Per cent of coverage and capacity sites

	Dedicated		*Commercial (one mobile carrier)*		*Commercial (two mobile carriers)*	
	Dense urban, urban and suburban	Rural and remote	Dense urban, urban and suburban	Rural and remote	Dense urban, urban and suburban	Rural and remote
Additional battery backup	100	100	100	100	75	75
Civil site upgrades	5	5	5	5	5	5

End-user devices

The number of end-user devices has been estimated using the total number of PSA users as a guide.

The Commission sought feedback on the scope of PSA users from participants. There was broad agreement that police, fire, ambulance, state emergency services and marine rescue and coast guard were captured by the terms of reference. Some participants considered that a broader cross-section of personnel should have access to PSMB (chapter 2). For the purposes of the quantitative analysis, it is assumed that police, fire, ambulance, and state emergency services (SES) would be the core users of this new capability.

Data from SCRGSP (2014) indicate that there are approximately 100 000 full-time equivalent public safety officers in Australia (approximately 65 000 police and 35 000 fire, ambulance and SES personnel in aggregate) and 250 000 volunteers across fire, ambulance and SES services.

Translating the number of officers into the number of devices requires assumptions about:

- the number of officers that take up a service and when this occurs within the period of analysis
- the type of device used (commercial handset, a ruggedised PSMB handset or an in-vehicle terminal, or multiple devices)
- the ratio between handheld devices and in-vehicle terminals, and how this differs depending on the type of PSA.

The following assumptions have been made in each category for the purposes of the quantitative analysis (table C.14).

Table C.14 **Number of PSA users and devices**

Variable	*Central case*
Number of users	100 000
Growth per annum in number of users	0
Handheld devices as a percentage of users	50
Ruggedised handsets as a percentage of users	50
In vehicle modems as a percentage of users	10

Core network items

As noted in section C.5, the number of core network items is generally specified as part of option design. Table C.15 sets out the number of units of each core network item required under each option and sub-option.

Table C.15 **Number of units for core network items**
By option and sub-option

Cost item	*1*	*2a, 3a*	*2b, 3b*	*2c, 3c*	*4a*	*4b*
National approach						
CoreNational	1	0	1	1	0	0
CoreState	0	0	0	0	0	0
PreferentialAccess	0	0	0	0	0	0
LMRIntegration	1	1	2	3	1	2
OSSBSS	1	0	1	1	0	0
State-based approach						
CoreNational	0	..	0	0	..	..
CoreState	8	..	8	8	..	..
PreferentialAccess	0	..	0	0	..	..
LMRIntegration	8	..	9	10	..	..
OSSBSS	8	..	8	8	..	..

.. Not applicable

Overflow traffic

Table C.16 outlines the proportion of total traffic that is assumed to overflow onto mobile carrier networks under each option. As discussed earlier, the proportion of overflow in rural and remote geotypes is always set to zero per cent, which is equivalent to specifying that no additional sites are required for overflow in these areas.

Table C.16 **Overflow traffic**
Per cent

	Dense urban	*Urban*	*Suburban*	*Rural*	*Remote*
Option 1	0	0	0	0	0
Option 2	20	20	20	0	0
Option 3	20	20	20	0	0
Option 4	100	100	100	0	0

Capital expenditure: unit costs

Sourcing accurate and robust values for unit costs is a difficult exercise. In part, this is because it is ‘difficult to estimate infrastructure costs beyond 3–5 years due to ongoing technology and capability enhancement’ (Ericsson, sub. 10, p. 22). In addition, there is limited publicly available information relating to unit costs and observed market prices may include a markup over the true resource cost.

Table C.17 sets out the assumed unit costs for capital expenditure items, expressed in real terms. While there is scope for the quantitative analysis to account for real price trends, it has been assumed for now that real prices remain constant over the evaluation period (that is, zero per cent change in real prices). The Commission will explore this further for the final report.

Table C.17 Unit costs for capital expenditure items

In 2015 dollars

Cost item	*Central case*	*Lower bound*	*Upper bound*
Radio access network			
NewSiteBuildMetro	300 000	150 000	450 000
NewSiteBuildRegional	300 000	150 000	450 000
SiteEquipment	80 000	50 000	120 000
Site hardening costs			
Battery20	10 000	..	..
Battery24	12 000	..	..
Civil	50 000	..	..
Core network and add-ons			
CoreNational	10 000 000	..	..
CoreState	7 500 000	..	..
PreferentialAccess	5 000 000	..	..
LMRIntegration	20 000 000	..	..
OSSBSS	50 000 000	..	..
User equipment			
Handset	800	..	..
RuggedisedHandset	2 500	..	..
IVModem	7 500	..	..
Mobile carrier network augmentation			
MNOSitesAugmentation	80 000	..	..
CoreNetworkAugmentation	15	..	..

.. Not applicable

Opportunity cost of spectrum

There are two broad approaches to calculating the opportunity cost of spectrum.

- *Market valuation approaches* calculate the value of spectrum using available market information or data as a benchmark. Most commonly, this involves the use of data from previous spectrum market transactions, such as past auction results and spectrum trades in the secondary market involving spectrum parcels in the same or similar band (Access Economics 2010; Grous 2013a, 2013b).
- *Direct calculation approaches* calculate the value of spectrum by reference to the cost and revenue advantages of acquiring spectrum. This is typically done by estimating the cost of other inputs needed to maintain a certain level and quality of output on a mobile network, but without the additional spectrum (NERA and Smith System Engineering 1996; Plum Consulting 2008).

For the purpose of the quantitative analysis, the opportunity cost of spectrum is estimated with reference to market transactions of spectrum in the same or comparable frequency bands. Compared to direct calculation methods, this approach has lower information requirements and is more transparent and objective.

Generally, there is limited publicly available data that can be used to infer the value of spectrum in Australia. Data relating to international valuations of spectrum (such as auction results) are of limited use, given that spectrum is not tradeable across geographical areas and its use is subject to different licencing conditions in different jurisdictions.

- In 2013, spectrum in the 700 MHz band was sold at auction for a reserve price of $1.36/MHz/Pop based on a Ministerial direction; and spectrum in the 2.5 GHz band was sold at $0.03/MHz/Pop based on an ACMA reserve price
- In their report to ACMA, Plum Consulting (2008) estimated that the opportunity cost of spectrum in 825–845 MHz and 870–890 MHz bands was $1.21–$1.46/MHz/Pop.
- Optus (sub. 18) submitted that the opportunity cost of spectrum in the 900 MHz, 800 MHz and 750 MHz ranges would likely be between $1.00–$1.36/MHz/pop.
- The ACMA Apparatus Licence Fee Schedule specifies that 900 MHz PMTS Class B licences are charged at $3 148 358/MHz, which roughly translates to $0.50/MHz/Pop, given the different lengths of the licences.

For the purpose of the quantitative analysis, guidance has been taken from these sources to establish an appropriate range (table C.18).

Table C.18 **Spectrum assumptions**

Item	*Central case*	*Lower bound*	*Upper bound*
Price per MHz per head of population	$1.00	$0.50	$1.36
Population[a]	22 872 578	..	..
Apportionment to dense urban, urban and suburban areas	85%	..	..
Apportionment to rural and remote areas	15%	..	..

[a] Estimated resident population as at 31 March 2013. This is the population count used by ACMA for setting the reserve price for the digital dividend auction. **..** Not applicable

Additionally, the opportunity cost of spectrum has been apportioned between dense urban, urban and suburban areas on the one hand and rural and remote areas on the other. This recognises that if a dedicated network only provides partial geographical coverage, the same spectrum bands could be used for other purposes in other areas (namely, rural and remote areas).

The estimates outlined in the table above are for the purposes of this quantitative analysis only, and should not be taken as a statement of the Commission's view on the appropriate price of spectrum, as this is a matter for the ACMA and the Minister for Communications.

Timing of capital expenditure

Parameters relating to the rollout of infrastructure and take-up schedules have been calibrated with reference to publicly available sources relating to rollout schedules for other LTE networks (table C.19). Assumptions relating to the length of rollout and asset life were calibrated on this basis and are detailed in table C.20.

Table C.19 **Rollout and take-up schedule**

Approach	*Build time*	*Sources*
Dedicated	5 years	Expected timeframe for Telstra LTE rollout for 99% of population (2011 to 2017)
Targeted hybrid	3 years	Telstra LTE rollout for up to 80% of population (2011 to 2013)
Commercial	2 years	..

.. Not applicable

Table C.20 **Rollout period and asset life spans**
Years

Cost item	*Rollout period (dedicated)*	*Rollout period (targeted hybrid)*	*Rollout period (commercial)*	*Asset life*
Radio access network				
NewSiteBuildMetro	5	3	..	20
NewSiteBuildRegional	5	3	..	20
SiteEquipment	5	3	..	8
Site hardening costs				
Battery20	..	3	2	8
Battery24	5	3	..	8
Civil	5	3	2	20
Core network and add-ons				
CoreNational	1	1	..	8
CoreState	1	1	..	8
PreferentialAccess	1	1	1	8
LMRIntegration	1	1	1	8
OSSBSS	1	1	..	8
User equipment				
Handset	5	5	5	3
RuggedisedHandset	5	5	5	5
IVModem	5	5	5	5
Spectrum				
Spectrum	1	1	..	15
Mobile carrier network augmentation				
MNOSitesAugmentation	..	1	1	8
CoreNetworkAugmentation	..	1	1	8

.. Not applicable

Operating costs

Direct network operating costs

As discussed above, direct network operating costs are estimated using expense ratios. Reliable data on expense ratios for LTE networks are difficult to source. SCF Associates (2014) approximated annual operating costs as 15 per cent of the networks' value in operation.

The expense ratios, including upper and lower bound estimates, used for the quantitative analysis are set out in table C.21.

Table C.21 **Direct network operating costs**
Percentage of unit costs

Cost item	*Central case*	*Lower bound*	*Upper bound*
Radio access network			
NewSiteBuildMetro	7.5	5.0	10.0
NewSiteBuildRegional	7.5	5.0	10.0
SiteEquipment	7.5	5.0	10.0
Site hardening costs			
Battery20	7.5	5.0	10.0
Battery24	7.5	5.0	10.0
Civil	0.0	0.0	0.0
Core network and add-ons			
CoreNational	7.5	5.0	10.0
CoreState	7.5	5.0	10.0
PreferentialAccess	7.5	5.0	10.0
LMRIntegration	7.5	5.0	10.0
OSSBSS	7.5	5.0	10.0
User equipment			
Handset	0.0	0.0	0.0
RuggedisedHandset	0.0	0.0	0.0
IVModem	0.0	0.0	0.0
Spectrum			
Spectrum	0.0	0.0	0.0
Mobile carrier network augmentation			
MNOSitesAugmentation	7.5	5.0	10.0
CoreNetworkAugmentation	7.5	5.0	10.0

Network support operating costs

Network support assets include annual site rental costs and the purchase of backhaul transmission capacity to carry traffic between individual sites and the core network.

Site Leasing

The parameters used for site leasing costs are set out in table C.22.

Table C.22 **Site leasing costs**
Dollars per year

Cost item	*Central case*	*Lower bound*	*Upper bound*
Network support operating costs			
SiteLeasingUrban[a]	20 000	15 000	25 000
SiteLeasingRegional[b]	12 500	10 000	20 000

[a] Applies to dense urban, urban and suburban areas. [b] Applies to rural and remote areas.

Backhaul transmission

For the purposes of the quantitative analysis, it has been assumed that backhaul capacity would be leased from the existing commercial market. Developing robust estimates for backhaul transmission capacity is challenging for a range of reasons.

In terms of estimating the *quantity* of backhaul transmission required, mobile carriers and state governments currently own and lease capacity on backhaul links for existing networks, including mobile, LMR and other networks (Victorian Government, sub. 28). As a result, the incremental capacity required will depend on the extent to which current backhaul capacity can be used, the number of users of PSMB, their expected traffic, and the amount of spectrum available (Motorola, sub. 12). It will also fundamentally depend on the topology of the backhaul network in place and where the points of aggregation (and the core network) are in relation to each site.

In terms of estimating *unit costs* of backhaul transmission, there is limited data relating to the incremental resource costs of providing capacity on a backhaul link and how these might differ across the options considered in this study. Regulated prices set by the ACCC provide a guide to carrier pricing of backhaul services. However, these prices may not reflect the prices commercially negotiated in the market, including where capacity is bought in bulk or leased over long periods of time.

Additionally, the unit cost of transmission technology will likely improve with higher capacity of usage. For example, optical fibre transmission has a high initial cost of construction regardless of whether the capacity being used is only relatively small. The marginal cost to increase capacity on the fibre by addition of more electronics is likely to be relatively small — hence the unit rate ($/Mbps/km) would decrease the higher the capacity of the link.

As discussed in section C.5, a simplified approach is taken to estimating the cost of backhaul transmission, via a representative per-site cost that captures backhaul capacity from each mobile site back to some point of aggregation (but not necessarily the core network), as well as an annualised cost for new backhaul links. This representative per-site cost is calibrated with reference to estimates cited in some publicly available studies on

PSMB (Bell Labs 2011; Nokia Siemens Network 2010), as well as draft ACCC regulated pricing (ACCC 2015a).

Per-site backhaul costs are based on the following assumptions:

- backhaul between urban sites requires an average link capacity of 75–100 Mbps, and sites are 5–10 km from the relevant point of aggregation
- backhaul between regional sites requires an average link capacity of 25–40 Mbps, and sites are 50–100 km from the relevant point of aggregation.

To account for the savings associated with higher usage and existing infrastructure, it is assumed that the cost of backhaul is lower when the PSMB capability is delivered over a commercial network (table C.23).

Table C.23 **Per-site backhaul transmission costs**
Dollars per year

Cost item	*Options*	*Central case*	*Lower bound*	*Upper bound*
Network support operating costs				
BackhaulUrban[a]	1, 2b, 2c, 3b, 3c	20 000	15 000	25 000
BackhaulRegional[b]	1, 2b, 2c, 3b, 3c	25 000	20 000	30 000
BackhaulUrban[a]	2a, 3a, 4a, 4b	14 000	10 500	17 500
BackhaulRegional[b]	2a, 3a, 4a, 4b	17 500	14 000	21 000

[a] Applies to dense urban, urban and suburban areas. [b] Applies to rural and remote areas.

It should also be noted that there are difficulties associated with forecasting backhaul requirements into the future, as technologies and costs will likely change over time. As such, while it is assumed that real prices and backhaul requirements are constant over the 20-year evaluation period, this may not be realistic.

C.7 Results

Table C.24 summarises the results of the quantitative analysis for the central case.

Table C.24 **Net present value of costs**

$ millions

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Total costs														
Total	6122.8	7539.0	5072.5	5774.9	7191.1	5784.6	7200.8	4335.8	4841.6	6257.8	4850.1	6266.3	2083.0	2107.2
Capital Expenditure														
NewSiteBuildMetro	70.7	70.7	60.8	60.8	60.8	60.8	60.8	65.9	65.9	65.9	65.9	65.9	0.0	0.0
NewSiteBuildRegional	39.9	39.9	39.9	39.9	39.9	39.9	39.9	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	1 039.3	1 039.3	947.1	947.1	947.1	947.1	947.1	626.0	626.0	626.0	626.0	626.0	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	51.6	51.6	51.6	38.7	38.7	103.0	77.3
Battery24	155.9	155.9	142.1	142.1	142.1	106.6	106.6	93.9	93.9	93.9	70.4	70.4	0.0	0.0
Civil	18.4	18.4	16.8	16.8	16.8	16.8	16.8	18.2	18.2	18.2	18.2	18.2	14.3	14.3
CoreNational	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	0.0
CoreState	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0
PreferentialAccess	8.4	67.4	8.4	16.9	75.9	25.3	84.3	8.4	16.9	75.9	25.3	84.3	8.4	16.9
LMRIntegration	33.7	269.7	33.7	67.4	303.4	101.1	337.1	33.7	67.4	303.4	101.1	337.1	33.7	67.4
OSSBSS	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	0.0
Handset	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2
RuggedisedHandset	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5
IVModem	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1
Spectrum	263.6	263.6	263.6	263.6	263.6	263.6	263.6	224.0	224.0	224.0	224.0	224.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	170.6	170.6
CoreNetworkAugmentation	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8
Total capital expenditure	2 265.7	3 228.2	2 082.5	2 225.8	3 188.3	2 232.4	3 194.9	1 691.9	1 835.2	2 797.7	1 841.0	2 803.5	864.8	881.2

[a] National approach. [b] State-by-state approach.

(continued next page)

Table C.24 (continued)

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Operating costs														
NewSiteBuildMetro	59.0	59.0	50.7	50.7	50.7	50.7	50.7	55.3	55.3	55.3	55.3	55.3	0.0	0.0
NewSiteBuildRegional	33.2	33.2	33.2	33.2	33.2	33.2	33.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	491.3	491.3	447.4	447.4	447.4	447.4	447.4	295.0	295.0	295.0	295.0	295.0	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	24.2	24.2	24.2	18.2	18.2	48.4	36.3
Battery24	73.7	73.7	67.1	67.1	67.1	50.3	50.3	44.2	44.2	44.2	33.2	33.2	0.0	0.0
Civil	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
CoreNational	7.9	0.0	0.0	7.9	0.0	7.9	0.0	0.0	7.9	0.0	7.9	0.0	0.0	0.0
CoreState	0.0	44.5	0.0	0.0	44.5	0.0	44.5	0.0	0.0	44.5	0.0	44.5	0.0	0.0
PreferentialAccess	4.0	31.8	4.0	7.9	35.8	11.9	39.7	4.0	7.9	35.8	11.9	39.7	4.0	7.9
LMRIntegration	15.9	127.1	15.9	31.8	143.0	47.7	158.9	15.9	31.8	143.0	47.7	158.9	15.9	31.8
OSSBSS	39.7	317.8	0.0	39.7	317.8	39.7	317.8	0.0	39.7	317.8	39.7	317.8	0.0	0.0
Handset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
RuggedisedHandset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
IVModem	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Spectrum	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	16.7	16.7	16.7	16.7	16.7	16.7	16.7	16.7	16.7	16.7	80.3	80.3
CoreNetworkAugmentation	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3
BackhaulUrban	1 048.1	1 048.1	631.1	901.5	901.5	901.5	901.5	688.3	983.3	983.3	983.3	983.3	456.8	456.8
BackhaulRegional	737.2	737.2	516.0	737.2	737.2	737.2	737.2	564.8	564.8	564.8	564.8	564.8	611.5	611.5
SiteLeasingUrban	995.7	995.7	856.5	856.5	856.5	856.5	856.5	934.1	934.1	934.1	934.1	934.1	0.0	0.0
SiteLeasingRegional	350.2	350.2	350.2	350.2	350.2	350.2	350.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Total operating costs	3 857.1	4 310.8	2 990.0	3 549.1	4 002.8	3 552.2	4 005.9	2 643.8	3 006.3	3 460.0	3 009.1	3 462.8	1 218.2	1 226.0

[a] National approach. [b] State-by-state approach.

C.8 Sensitivity testing

This section details the sensitivity testing that has been undertaken to understand how the results of the quantitative analysis change in response to changes in variables and assumptions.

There are a variety of approaches to sensitivity analysis (box C.7). Of these, the partial sensitivity analysis and a modified worst-case analysis were undertaken, on the basis of available information.

While a full risk analysis would provide more comprehensive results, its results would be largely driven by the probability distributions assigned to input values. In other words, the robustness of the analysis is dependent on the accuracy of the assumed distributions, for which data are lacking or insufficient in this case.

Box C.7 Approaches to sensitivity analysis

Depending on the nature and extent of the risk and uncertainty associated with a project, different approaches to sensitivity analysis could be used.

- *Worst-case scenario analysis*. The first step is to construct a hypothetical worst-case scenario by identifying the least favourable plausible outcome for each variable, and calculating results using those values.
- *Partial sensitivity analysis*. If there are a small number of key variables, an analysis of how the results are affected by changes in the most important variables may be sufficient.
- *Full risk analysis*. When there are many uncertain variables, it may be necessary to undertake a full risk analysis (using, for example, Monte Carlo simulation). This involves assigning probabilities to the values of all key variables and assigning covariances for pairs or sets of variables. A probability distribution of the results is then generated through random sampling of the values of the variables. This provides a comprehensive analysis of the potential variability of the results.

Sources: Department of Finance and Administration (2006); PC (2014b).

Partial sensitivity analysis

The partial sensitivity analysis was conducted by varying the input value of one variable at a time and holding all other values constant. Eleven different variables were varied, using upper and lower bounds, yielding 21 sets of results.

This section presents the results of the partial sensitivity analysis, as follows:

- tables C.25 and C.26: lower and upper bound values for the discount rate
- tables C.27 and C.28: lower and upper bound values for traffic volumes
- tables C.29 and C.30: lower and upper bound values for traffic growth
- table C.31: upper bound value for the quantum of dedicated spectrum
- tables C.32 and C.33: lower and upper bound values for the opportunity cost of spectrum
- tables C.34 and C.35: lower and upper bound values for the cost of site equipment
- tables C.36 and C.37: lower and upper bound values for the number of greenfield sites
- tables C.38 and C.39: lower and upper bound values for the cost of greenfield site builds
- tables C.40 and C.41: lower and upper bound values for network operating costs
- tables C.42 and C.43: lower and upper bound values for site leasing costs
- tables C.44 and C.45: lower and upper bound values for backhaul rental costs.

Table C.25 **Net present value of costs (lower bound discount rate)**
$ millions

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Total costs														
Total	8 583.9	10 411.6	7 073.1	8 070.0	9 897.7	8 079.3	9 906.9	5 972.2	6 671.3	8 498.9	6 680.4	8 508.0	2 857.8	2 888.4
Capital Expenditure														
NewSiteBuildMetro	77.1	77.1	66.3	66.3	66.3	66.3	66.3	70.5	70.5	70.5	70.5	70.5	0.0	0.0
NewSiteBuildRegional	43.2	43.2	43.2	43.2	43.2	43.2	43.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	1 348.8	1 348.8	1 228.6	1 228.6	1 228.6	1 228.6	1 228.6	797.0	797.0	797.0	797.0	797.0	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	65.3	65.3	65.3	49.0	49.0	128.9	96.7
Battery24	202.3	202.3	184.3	184.3	184.3	138.2	138.2	119.5	119.5	119.5	89.7	89.7	0.0	0.0
Civil	20.0	20.0	18.2	18.2	18.2	18.2	18.2	19.4	19.4	19.4	19.4	19.4	15.0	15.0
CoreNational	20.9	0.0	0.0	20.9	0.0	20.9	0.0	0.0	20.9	0.0	20.9	0.0	0.0	0.0
CoreState	0.0	116.8	0.0	0.0	116.8	0.0	116.8	0.0	0.0	116.8	0.0	116.8	0.0	0.0
PreferentialAccess	10.4	83.4	10.4	20.9	93.8	31.3	104.3	10.4	20.9	93.8	31.3	104.3	10.4	20.9
LMRIntegration	41.7	333.6	41.7	83.4	375.3	125.1	417.0	41.7	83.4	375.3	125.1	417.0	41.7	83.4
OSSBSS	104.3	834.0	0.0	104.3	834.0	104.3	834.0	0.0	104.3	834.0	104.3	834.0	0.0	0.0
Handset	178.6	178.6	178.6	178.6	178.6	178.6	178.6	178.6	178.6	178.6	178.6	178.6	178.6	178.6
RuggedisedHandset	345.8	345.8	345.8	345.8	345.8	345.8	345.8	345.8	345.8	345.8	345.8	345.8	345.8	345.8
IVModem	207.5	207.5	207.5	207.5	207.5	207.5	207.5	207.5	207.5	207.5	207.5	207.5	207.5	207.5
Spectrum	292.6	292.6	292.6	292.6	292.6	292.6	292.6	248.7	248.7	248.7	248.7	248.7	0.0	0.0
MNOSitesAugmentation	0.0	0.0	44.3	44.3	44.3	44.3	44.3	44.3	44.3	44.3	44.3	44.3	213.4	213.4
CoreNetworkAugmentation	3.4	3.4	3.4	3.4	3.4	3.4	3.4	3.4	3.4	3.4	3.4	3.4	3.4	3.4
Total capital expenditure	2 896.6	4 087.2	2 665.0	2 842.2	4 032.8	2 848.3	4 038.9	2 152.2	2 329.4	3 520.0	2 335.3	3 525.9	1 144.8	1 164.7

[a] National approach. [b] State-by-state approach.

(continued next page)

Table C.25 (continued)

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Operating costs														
NewSiteBuildMetro	87.2	87.2	75.0	75.0	75.0	75.0	75.0	80.1	80.1	80.1	80.1	80.1	0.0	0.0
NewSiteBuildRegional	48.7	48.7	48.7	48.7	48.7	48.7	48.7	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	725.1	725.1	659.9	659.9	659.9	659.9	659.9	427.0	427.0	427.0	427.0	427.0	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	34.8	34.8	34.8	26.1	26.1	68.8	51.6
Battery24	108.8	108.8	99.0	99.0	99.0	74.2	74.2	64.1	64.1	64.1	48.0	48.0	0.0	0.0
Civil	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
CoreNational	11.2	0.0	0.0	11.2	0.0	11.2	0.0	0.0	11.2	0.0	11.2	0.0	0.0	0.0
CoreState	0.0	62.5	0.0	0.0	62.5	0.0	62.5	0.0	0.0	62.5	0.0	62.5	0.0	0.0
PreferentialAccess	5.6	44.6	5.6	11.2	50.2	16.7	55.8	5.6	11.2	50.2	16.7	55.8	5.6	11.2
LMRIntegration	22.3	178.5	22.3	44.6	200.8	66.9	223.2	22.3	44.6	200.8	66.9	223.2	22.3	44.6
OSSBSS	55.8	446.3	0.0	55.8	446.3	55.8	446.3	0.0	55.8	446.3	55.8	446.3	0.0	0.0
Handset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
RuggedisedHandset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
IVModem	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Spectrum	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	23.7	23.7	23.7	23.7	23.7	23.7	23.7	23.7	23.7	23.7	114.1	114.1
CoreNetworkAugmentation	1.8	1.8	1.8	1.8	1.8	1.8	1.8	1.8	1.8	1.8	1.8	1.8	1.8	1.8
BackhaulUrban	1 550.4	1 550.4	933.1	1 333.0	1 333.0	1 333.0	1 333.0	996.3	1 423.3	1 423.3	1 423.3	1 423.3	641.5	641.5
BackhaulRegional	1 083.1	1 083.1	758.2	1 083.1	1 083.1	1 083.1	1 083.1	812.1	812.1	812.1	812.1	812.1	858.8	858.8
SiteLeasingUrban	1 472.9	1 472.9	1 266.4	1 266.4	1 266.4	1 266.4	1 266.4	1 352.2	1 352.2	1 352.2	1 352.2	1 352.2	0.0	0.0
SiteLeasingRegional	514.5	514.5	514.5	514.5	514.5	514.5	514.5	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Total operating costs	5 687.3	6 324.4	4 408.1	5 227.8	5 864.9	5 231.0	5 868.1	3 820.0	4 341.8	4 979.0	4 345.0	4 982.1	1 712.9	1 723.6

[a] National approach. [b] State-by-state approach.

Table C.26 **Net present value of costs (upper bound discount rate)**
$ millions

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Total costs														
Total	4 585.2	5 733.2	3 816.8	4 338.6	5 486.6	4 348.6	5 496.6	3 306.8	3 692.5	4 840.5	3 700.7	4 848.7	1 596.7	1 616.7
Capital Expenditure														
NewSiteBuildMetro	64.1	64.1	55.2	55.2	55.2	55.2	55.2	61.3	61.3	61.3	61.3	61.3	0.0	0.0
NewSiteBuildRegional	36.5	36.5	36.5	36.5	36.5	36.5	36.5	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	826.6	826.6	753.6	753.6	753.6	753.6	753.6	508.2	508.2	508.2	508.2	508.2	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	42.1	42.1	42.1	31.6	31.6	85.2	63.9
Battery24	124.0	124.0	113.0	113.0	113.0	84.8	84.8	76.2	76.2	76.2	57.2	57.2	0.0	0.0
Civil	16.8	16.8	15.3	15.3	15.3	15.3	15.3	17.0	17.0	17.0	17.0	17.0	13.6	13.6
CoreNational	14.1	0.0	0.0	14.1	0.0	14.1	0.0	0.0	14.1	0.0	14.1	0.0	0.0	0.0
CoreState	0.0	79.1	0.0	0.0	79.1	0.0	79.1	0.0	0.0	79.1	0.0	79.1	0.0	0.0
PreferentialAccess	7.1	56.5	7.1	14.1	63.6	21.2	70.7	7.1	14.1	63.6	21.2	70.7	7.1	14.1
LMRIntegration	28.3	226.1	28.3	56.5	254.4	84.8	282.7	28.3	56.5	254.4	84.8	282.7	28.3	56.5
OSSBSS	70.7	565.3	0.0	70.7	565.3	70.7	565.3	0.0	70.7	565.3	70.7	565.3	0.0	0.0
Handset	93.5	93.5	93.5	93.5	93.5	93.5	93.5	93.5	93.5	93.5	93.5	93.5	93.5	93.5
RuggedisedHandset	194.0	194.0	194.0	194.0	194.0	194.0	194.0	194.0	194.0	194.0	194.0	194.0	194.0	194.0
IVModem	116.4	116.4	116.4	116.4	116.4	116.4	116.4	116.4	116.4	116.4	116.4	116.4	116.4	116.4
Spectrum	238.0	238.0	238.0	238.0	238.0	238.0	238.0	202.3	202.3	202.3	202.3	202.3	0.0	0.0
MNOSitesAugmentation	0.0	0.0	29.4	29.4	29.4	29.4	29.4	29.4	29.4	29.4	29.4	29.4	141.6	141.6
CoreNetworkAugmentation	2.3	2.3	2.3	2.3	2.3	2.3	2.3	2.3	2.3	2.3	2.3	2.3	2.3	2.3
Total capital expenditure	1 832.3	2 639.3	1 682.6	1 802.8	2 609.8	1 809.9	2 616.9	1 378.2	1 498.3	2 305.3	1 504.0	2 311.1	682.1	696.1

[a] National approach. [b] State-by-state approach.

(continued next page)

Table C.26 (continued)

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Operating costs														
NewSiteBuildMetro	41.9	41.9	36.1	36.1	36.1	36.1	36.1	40.3	40.3	40.3	40.3	40.3	0.0	0.0
NewSiteBuildRegional	23.7	23.7	23.7	23.7	23.7	23.7	23.7	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	350.4	350.4	319.2	319.2	319.2	319.2	319.2	214.8	214.8	214.8	214.8	214.8	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	17.7	17.7	17.7	13.3	13.3	35.9	27.0
Battery24	52.6	52.6	47.9	47.9	47.9	35.9	35.9	32.2	32.2	32.2	24.2	24.2	0.0	0.0
Civil	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
CoreNational	6.0	0.0	0.0	6.0	0.0	6.0	0.0	0.0	6.0	0.0	6.0	0.0	0.0	0.0
CoreState	0.0	33.4	0.0	0.0	33.4	0.0	33.4	0.0	0.0	33.4	0.0	33.4	0.0	0.0
PreferentialAccess	3.0	23.9	3.0	6.0	26.9	9.0	29.9	3.0	6.0	26.9	9.0	29.9	3.0	6.0
LMRIntegration	11.9	95.6	11.9	23.9	107.5	35.8	119.4	11.9	23.9	107.5	35.8	119.4	11.9	23.9
OSSBSS	29.9	238.9	0.0	29.9	238.9	29.9	238.9	0.0	29.9	238.9	29.9	238.9	0.0	0.0
Handset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
RuggedisedHandset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
IVModem	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Spectrum	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	12.4	12.4	12.4	12.4	12.4	12.4	12.4	12.4	12.4	12.4	59.7	59.7
CoreNetworkAugmentation	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
BackhaulUrban	745.7	745.7	449.2	641.7	641.7	641.7	641.7	501.2	716.0	716.0	716.0	716.0	343.4	343.4
BackhaulRegional	527.7	527.7	369.4	527.7	527.7	527.7	527.7	413.8	413.8	413.8	413.8	413.8	459.6	459.6
SiteLeasingUrban	708.4	708.4	609.6	609.6	609.6	609.6	609.6	680.2	680.2	680.2	680.2	680.2	0.0	0.0
SiteLeasingRegional	250.7	250.7	250.7	250.7	250.7	250.7	250.7	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Total operating costs	2 752.9	3 093.9	2 134.2	2 535.8	2 876.8	2 538.7	2 879.8	1 928.6	2 194.2	2 535.2	2 196.6	2 537.6	914.6	920.6

[a] National approach. [b] State-by-state approach.

Table C.27 **Net present value of costs (lower bound traffic volumes)**

$ millions

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Total costs														
Total	5 345.5	6 761.7	4 492.2	5 135.1	6 551.4	5 151.7	6 568.0	3 708.5	4 150.5	5 566.7	4 166.6	5 582.8	1 999.9	2 024.1
Capital Expenditure														
NewSiteBuildMetro	54.2	54.2	47.7	47.7	47.7	47.7	47.7	51.6	51.6	51.6	51.6	51.6	0.0	0.0
NewSiteBuildRegional	39.7	39.7	39.7	39.7	39.7	39.7	39.7	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	884.2	884.2	822.7	822.7	822.7	822.7	822.7	491.0	491.0	491.0	491.0	491.0	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	51.4	51.4	51.4	38.6	38.6	103.0	77.3
Battery24	132.6	132.6	123.4	123.4	123.4	92.6	92.6	73.6	73.6	73.6	55.2	55.2	0.0	0.0
Civil	15.7	15.7	14.6	14.6	14.6	14.6	14.6	15.8	15.8	15.8	15.8	15.8	14.3	14.3
CoreNational	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	0.0
CoreState	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0
PreferentialAccess	8.4	67.4	8.4	16.9	75.9	25.3	84.3	8.4	16.9	75.9	25.3	84.3	8.4	16.9
LMRIntegration	33.7	269.7	33.7	67.4	303.4	101.1	337.1	33.7	67.4	303.4	101.1	337.1	33.7	67.4
OSSBSS	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	0.0
Handset	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2
RuggedisedHandset	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5
IVModem	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1
Spectrum	263.6	263.6	263.6	263.6	263.6	263.6	263.6	224.0	224.0	224.0	224.0	224.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	24.3	24.3	24.3	24.3	24.3	24.3	24.3	24.3	24.3	24.3	114.3	114.3
CoreNetworkAugmentation	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8
Total capital expenditure	2 068.0	3 030.5	1 912.8	2 056.0	3 018.6	2 067.3	3 029.9	1 508.6	1 651.9	2 614.4	1 662.8	2 625.3	808.5	824.9

[a] National approach. [b] State-by-state approach.

(continued next page)

Table C.27 (continued)

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Operating costs														
NewSiteBuildMetro	45.2	45.2	39.7	39.7	39.7	39.7	39.7	43.3	43.3	43.3	43.3	43.3	0.0	0.0
NewSiteBuildRegional	33.0	33.0	33.0	33.0	33.0	33.0	33.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	417.4	417.4	388.1	388.1	388.1	388.1	388.1	231.2	231.2	231.2	231.2	231.2	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	24.1	24.1	24.1	18.1	18.1	48.4	36.3
Battery24	62.6	62.6	58.2	58.2	58.2	43.7	43.7	34.7	34.7	34.7	26.0	26.0	0.0	0.0
Civil	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
CoreNational	7.9	0.0	0.0	7.9	0.0	7.9	0.0	0.0	7.9	0.0	7.9	0.0	0.0	0.0
CoreState	0.0	44.5	0.0	0.0	44.5	0.0	44.5	0.0	0.0	44.5	0.0	44.5	0.0	0.0
PreferentialAccess	4.0	31.8	4.0	7.9	35.8	11.9	39.7	4.0	7.9	35.8	11.9	39.7	4.0	7.9
LMRIntegration	15.9	127.1	15.9	31.8	143.0	47.7	158.9	15.9	31.8	143.0	47.7	158.9	15.9	31.8
OSSBSS	39.7	317.8	0.0	39.7	317.8	39.7	317.8	0.0	39.7	317.8	39.7	317.8	0.0	0.0
Handset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
RuggedisedHandset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
IVModem	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Spectrum	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	11.4	11.4	11.4	11.4	11.4	11.4	11.4	11.4	11.4	11.4	53.8	53.8
CoreNetworkAugmentation	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3
BackhaulUrban	803.8	803.8	494.3	706.1	706.1	706.1	706.1	539.4	770.6	770.6	770.6	770.6	456.8	456.8
BackhaulRegional	734.2	734.2	514.0	734.2	734.2	734.2	734.2	562.6	562.6	562.6	562.6	562.6	611.2	611.2
SiteLeasingUrban	763.6	763.6	670.8	670.8	670.8	670.8	670.8	732.0	732.0	732.0	732.0	732.0	0.0	0.0
SiteLeasingRegional	348.8	348.8	348.8	348.8	348.8	348.8	348.8	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Total operating costs	3 277.5	3 731.2	2 579.5	3 079.1	3 532.8	3 084.4	3 538.1	2 199.9	2 498.6	2 952.3	2 503.8	2 957.5	1 191.5	1 199.2

[a] National approach. [b] State-by-state approach.

Table C.28 **Net present value of costs (upper bound traffic volumes)**

$ millions

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Total costs														
Total	10 401.6	11 817.8	8 121.3	9 137.0	10 553.2	9 110.5	10 526.7	7 630.6	8 472.1	9 888.3	8 441.1	9 857.3	2 498.9	2 019.9
Capital Expenditure														
NewSiteBuildMetro	161.3	161.3	130.1	130.1	130.1	130.1	130.1	141.1	141.1	141.1	141.1	141.1	0.0	0.0
NewSiteBuildRegional	40.7	40.7	40.7	40.7	40.7	40.7	40.7	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	1 891.4	1 891.4	1 599.9	1 599.9	1 599.9	1 599.9	1 599.9	1 335.4	1 335.4	1 335.4	1 335.4	1 335.4	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	52.6	52.6	52.6	39.5	39.5	103.1	79.5
Battery24	283.7	283.7	240.0	240.0	240.0	180.0	180.0	200.3	200.3	200.3	150.2	150.2	0.0	0.0
Civil	33.7	33.7	28.5	28.5	28.5	28.5	28.5	30.9	30.9	30.9	30.9	30.9	14.3	14.7
CoreNational	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	0.0
CoreState	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0
PreferentialAccess	8.4	67.4	8.4	16.9	75.9	25.3	84.3	8.4	16.9	75.9	25.3	84.3	8.4	0.0
LMRIntegration	33.7	269.7	33.7	67.4	303.4	101.1	337.1	33.7	67.4	303.4	101.1	337.1	33.7	67.4
OSSBSS	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	0.0
Handset	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2
RuggedisedHandset	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	304.2
IVModem	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	76.1
Spectrum	263.6	263.6	263.6	263.6	263.6	263.6	263.6	224.0	224.0	224.0	224.0	224.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	91.8	91.8	91.8	91.8	91.8	91.8	91.8	91.8	91.8	91.8	452.4	452.4
CoreNetworkAugmentation	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8
Total capital expenditure	3 352.2	4 314.8	2 971.2	3 114.5	4 077.0	3 096.7	4 059.2	2 653.0	2 796.2	3 758.8	2 775.1	3 737.7	1 146.7	1 123.4

[a] National approach. [b] State-by-state approach.

(continued next page)

Table C.28 (continued)

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Operating costs														
NewSiteBuildMetro	134.7	134.7	108.6	108.6	108.6	108.6	108.6	118.3	118.3	118.3	118.3	118.3	0.0	0.0
NewSiteBuildRegional	33.8	33.8	33.8	33.8	33.8	33.8	33.8	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	898.8	898.8	759.7	759.7	759.7	759.7	759.7	630.7	630.7	630.7	630.7	630.7	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	24.7	24.7	24.7	18.5	18.5	48.5	37.5
Battery24	134.8	134.8	114.0	114.0	114.0	85.5	85.5	94.6	94.6	94.6	71.0	71.0	0.0	0.0
Civil	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
CoreNational	7.9	0.0	0.0	7.9	0.0	7.9	0.0	0.0	7.9	0.0	7.9	0.0	0.0	0.0
CoreState	0.0	44.5	0.0	0.0	44.5	0.0	44.5	0.0	0.0	44.5	0.0	44.5	0.0	0.0
PreferentialAccess	4.0	31.8	4.0	7.9	35.8	11.9	39.7	4.0	7.9	35.8	11.9	39.7	4.0	0.0
LMRIntegration	15.9	127.1	15.9	31.8	143.0	47.7	158.9	15.9	31.8	143.0	47.7	158.9	15.9	31.8
OSSBSS	39.7	317.8	0.0	39.7	317.8	39.7	317.8	0.0	39.7	317.8	39.7	317.8	0.0	0.0
Handset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
RuggedisedHandset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
IVModem	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Spectrum	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	43.2	43.2	43.2	43.2	43.2	43.2	43.2	43.2	43.2	43.2	212.9	212.9
CoreNetworkAugmentation	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3
BackhaulUrban	2 394.5	2 394.5	1 351.7	1 931.0	1 931.0	1 931.0	1 931.0	1 471.7	2 102.4	2 102.4	2 102.4	2 102.4	456.8	137.0
BackhaulRegional	751.9	751.9	526.3	751.9	751.9	751.9	751.9	576.0	576.0	576.0	576.0	576.0	612.7	476.0
SiteLeasingUrban	2 274.8	2 274.8	1 834.4	1 834.4	1 834.4	1 834.4	1 834.4	1 997.3	1 997.3	1 997.3	1 997.3	1 997.3	0.0	0.0
SiteLeasingRegional	357.2	357.2	357.2	357.2	357.2	357.2	357.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Total operating costs	7 049.4	7 503.1	5 150.1	6 022.5	6 476.2	6 013.8	6 467.5	4 977.6	5 675.9	6 129.6	5 665.9	6 119.6	1 352.2	896.5

[a] National approach. [b] State-by-state approach.

Table C.29 **Net present value of costs (lower bound traffic growth)**

$ millions

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Total costs														
Total	5 637.4	7 053.6	4 712.6	5 376.3	6 792.5	5 389.9	6 806.1	3 962.1	4 429.0	5 845.2	4 441.8	5 858.0	2 035.6	2 059.7
Capital Expenditure														
NewSiteBuildMetro	60.5	60.5	52.7	52.7	52.7	52.7	52.7	56.9	56.9	56.9	56.9	56.9	0.0	0.0
NewSiteBuildRegional	39.8	39.8	39.8	39.8	39.8	39.8	39.8	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	956.1	956.1	880.3	880.3	880.3	880.3	880.3	551.2	551.2	551.2	551.2	551.2	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	51.5	51.5	51.5	38.6	38.6	103.0	77.3
Battery24	143.4	143.4	132.1	132.1	132.1	99.0	99.0	82.7	82.7	82.7	62.0	62.0	0.0	0.0
Civil	16.7	16.7	15.4	15.4	15.4	15.4	15.4	16.7	16.7	16.7	16.7	16.7	14.3	14.3
CoreNational	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	0.0
CoreState	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0
PreferentialAccess	8.4	67.4	8.4	16.9	75.9	25.3	84.3	8.4	16.9	75.9	25.3	84.3	8.4	16.9
LMRIntegration	33.7	269.7	33.7	67.4	303.4	101.1	337.1	33.7	67.4	303.4	101.1	337.1	33.7	67.4
OSSBSS	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	0.0
Handset	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2
RuggedisedHandset	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5
IVModem	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1
Spectrum	263.6	263.6	263.6	263.6	263.6	263.6	263.6	224.0	224.0	224.0	224.0	224.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	29.0	29.0	29.0	29.0	29.0	29.0	29.0	29.0	29.0	29.0	138.3	138.3
CoreNetworkAugmentation	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8
Total capital expenditure	2 158.0	3 120.5	1 989.7	2 133.0	3 095.5	2 142.1	3 104.6	1 588.8	1 732.1	2 694.6	1 740.7	2 703.2	832.4	848.8

[a] National approach. [b] State-by-state approach.

(continued next page)

Table C.29 (continued)

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Operating costs														
NewSiteBuildMetro	50.0	50.0	43.5	43.5	43.5	43.5	43.5	48.0	48.0	48.0	48.0	48.0	0.0	0.0
NewSiteBuildRegional	33.1	33.1	33.1	33.1	33.1	33.1	33.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	443.1	443.1	408.7	408.7	408.7	408.7	408.7	256.1	256.1	256.1	256.1	256.1	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	24.1	24.1	24.1	18.1	18.1	48.4	36.3
Battery24	66.5	66.5	61.3	61.3	61.3	46.0	46.0	38.4	38.4	38.4	28.8	28.8	0.0	0.0
Civil	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
CoreNational	7.9	0.0	0.0	7.9	0.0	7.9	0.0	0.0	7.9	0.0	7.9	0.0	0.0	0.0
CoreState	0.0	44.5	0.0	0.0	44.5	0.0	44.5	0.0	0.0	44.5	0.0	44.5	0.0	0.0
PreferentialAccess	4.0	31.8	4.0	7.9	35.8	11.9	39.7	4.0	7.9	35.8	11.9	39.7	4.0	7.9
LMRIntegration	15.9	127.1	15.9	31.8	143.0	47.7	158.9	15.9	31.8	143.0	47.7	158.9	15.9	31.8
OSSBSS	39.7	317.8	0.0	39.7	317.8	39.7	317.8	0.0	39.7	317.8	39.7	317.8	0.0	0.0
Handset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
RuggedisedHandset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
IVModem	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Spectrum	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	13.7	13.7	13.7	13.7	13.7	13.7	13.7	13.7	13.7	13.7	65.4	65.4
CoreNetworkAugmentation	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3
BackhaulUrban	888.9	888.9	541.9	774.2	774.2	774.2	774.2	597.5	853.5	853.5	853.5	853.5	456.8	456.8
BackhaulRegional	735.3	735.3	514.7	735.3	735.3	735.3	735.3	563.4	563.4	563.4	563.4	563.4	611.4	611.4
SiteLeasingUrban	844.4	844.4	735.5	735.5	735.5	735.5	735.5	810.9	810.9	810.9	810.9	810.9	0.0	0.0
SiteLeasingRegional	349.3	349.3	349.3	349.3	349.3	349.3	349.3	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Total operating costs	3 479.4	3 933.1	2 722.9	3 243.3	3 697.0	3 247.8	3 701.5	2 373.3	2 696.9	3 150.6	2 701.2	3 154.8	1 203.2	1 210.9

[a] National approach. [b] State-by-state approach.

Table C.30 **Net present value of costs (upper bound traffic growth)**

$ millions

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Total costs														
Total	7 404.1	8 820.3	5 994.3	6 796.7	8 212.9	6 796.4	8 212.6	5 293.2	5 898.7	7 314.9	5 896.2	7 312.4	2 204.3	2 228.5
Capital Expenditure														
NewSiteBuildMetro	98.6	98.6	82.4	82.4	82.4	82.4	82.4	90.6	90.6	90.6	90.6	90.6	0.0	0.0
NewSiteBuildRegional	40.1	40.1	40.1	40.1	40.1	40.1	40.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	1 252.6	1 252.6	1 113.6	1 113.6	1 113.6	1 113.6	1 113.6	816.3	816.3	816.3	816.3	816.3	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	51.9	51.9	51.9	38.9	38.9	103.1	77.3
Battery24	187.9	187.9	167.0	167.0	167.0	125.3	125.3	122.4	122.4	122.4	91.8	91.8	0.0	0.0
Civil	23.1	23.1	20.4	20.4	20.4	20.4	20.4	22.3	22.3	22.3	22.3	22.3	14.3	14.3
CoreNational	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	0.0
CoreState	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0
PreferentialAccess	8.4	67.4	8.4	16.9	75.9	25.3	84.3	8.4	16.9	75.9	25.3	84.3	8.4	16.9
LMRIntegration	33.7	269.7	33.7	67.4	303.4	101.1	337.1	33.7	67.4	303.4	101.1	337.1	33.7	67.4
OSSBSS	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	0.0
Handset	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2
RuggedisedHandset	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5
IVModem	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1
Spectrum	263.6	263.6	263.6	263.6	263.6	263.6	263.6	224.0	224.0	224.0	224.0	224.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	52.0	52.0	52.0	52.0	52.0	52.0	52.0	52.0	52.0	52.0	253.7	253.7
CoreNetworkAugmentation	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8
Total capital expenditure	2 543.9	3 506.5	2 316.0	2 459.3	3 421.8	2 459.7	3 422.2	1 956.3	2 099.6	3 062.1	2 098.2	3 060.7	947.9	964.3

[a] National approach. [b] State-by-state approach.

(continued next page)

Table C.30 (continued)

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Operating costs														
NewSiteBuildMetro	82.7	82.7	69.2	69.2	69.2	69.2	69.2	74.0	74.0	74.0	74.0	74.0	0.0	0.0
NewSiteBuildRegional	33.4	33.4	33.4	33.4	33.4	33.4	33.4	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	619.4	619.4	547.1	547.1	547.1	547.1	547.1	394.7	394.7	394.7	394.7	394.7	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	24.4	24.4	24.4	18.3	18.3	48.5	36.3
Battery24	92.9	92.9	82.1	82.1	82.1	61.5	61.5	59.2	59.2	59.2	44.4	44.4	0.0	0.0
Civil	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
CoreNational	7.9	0.0	0.0	7.9	0.0	7.9	0.0	0.0	7.9	0.0	7.9	0.0	0.0	0.0
CoreState	0.0	44.5	0.0	0.0	44.5	0.0	44.5	0.0	0.0	44.5	0.0	44.5	0.0	0.0
PreferentialAccess	4.0	31.8	4.0	7.9	35.8	11.9	39.7	4.0	7.9	35.8	11.9	39.7	4.0	7.9
LMRIntegration	15.9	127.1	15.9	31.8	143.0	47.7	158.9	15.9	31.8	143.0	47.7	158.9	15.9	31.8
OSSBSS	39.7	317.8	0.0	39.7	317.8	39.7	317.8	0.0	39.7	317.8	39.7	317.8	0.0	0.0
Handset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
RuggedisedHandset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
IVModem	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Spectrum	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	24.2	24.2	24.2	24.2	24.2	24.2	24.2	24.2	24.2	24.2	118.1	118.1
CoreNetworkAugmentation	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3
BackhaulUrban	1 470.9	1 470.9	860.9	1 229.9	1 229.9	1 229.9	1 229.9	921.0	1 315.7	1 315.7	1 315.7	1 315.7	456.8	456.8
BackhaulRegional	742.1	742.1	519.5	742.1	742.1	742.1	742.1	568.3	568.3	568.3	568.3	568.3	611.9	611.9
SiteLeasingUrban	1 397.4	1 397.4	1 168.4	1 168.4	1 168.4	1 168.4	1 168.4	1 249.9	1 249.9	1 249.9	1 249.9	1 249.9	0.0	0.0
SiteLeasingRegional	352.5	352.5	352.5	352.5	352.5	352.5	352.5	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Total operating costs	4 860.1	5 313.8	3 678.3	4 337.4	4 791.1	4 336.7	4 790.4	3 336.8	3 799.1	4 252.7	3 798.0	4 251.7	1 256.4	1 264.2

[a] National approach. [b] State-by-state approach.

Table C.31 **Net present value of costs (upper bound quantum of spectrum)**
$ millions

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Total costs														
Total	5 220.3	6 636.6	4 490.3	5 103.5	6 519.7	5 123.5	6 539.7	3 643.5	4 053.6	5 469.8	4 073.4	5 489.6	2 083.0	1 604.0
Capital Expenditure														
NewSiteBuildMetro	46.0	46.0	41.1	41.1	41.1	41.1	41.1	44.5	44.5	44.5	44.5	44.5	0.0	0.0
NewSiteBuildRegional	39.6	39.6	39.6	39.6	39.6	39.6	39.6	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	806.6	806.6	760.5	760.5	760.5	760.5	760.5	423.4	423.4	423.4	423.4	423.4	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	51.3	51.3	51.3	38.5	38.5	103.0	79.4
Battery24	121.0	121.0	114.1	114.1	114.1	85.6	85.6	63.5	63.5	63.5	47.6	47.6	0.0	0.0
Civil	14.3	14.3	13.5	13.5	13.5	13.5	13.5	14.6	14.6	14.6	14.6	14.6	14.3	14.7
CoreNational	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	0.0
CoreState	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0
PreferentialAccess	8.4	67.4	8.4	16.9	75.9	25.3	84.3	8.4	16.9	75.9	25.3	84.3	8.4	0.0
LMRIntegration	33.7	269.7	33.7	67.4	303.4	101.1	337.1	33.7	67.4	303.4	101.1	337.1	33.7	67.4
OSSBSS	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	0.0
Handset	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2
RuggedisedHandset	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	304.2
IVModem	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	76.1
Spectrum	527.1	527.1	527.1	527.1	527.1	527.1	527.1	448.1	448.1	448.1	448.1	448.1	0.0	0.0
MNOSitesAugmentation	0.0	0.0	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	170.6	170.6
CoreNetworkAugmentation	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8
Total capital expenditure	2 232.6	3 195.1	2 108.2	2 251.4	3 214.0	2 265.1	3 227.6	1 657.7	1 801.0	2 763.5	1 814.4	2 776.9	864.8	841.4

[a] National approach. [b] State-by-state approach.

(continued next page)

Table C.31 (continued)

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Operating costs														
NewSiteBuildMetro	38.3	38.3	34.2	34.2	34.2	34.2	34.2	37.4	37.4	37.4	37.4	37.4	0.0	0.0
NewSiteBuildRegional	33.0	33.0	33.0	33.0	33.0	33.0	33.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	380.4	380.4	358.4	358.4	358.4	358.4	358.4	199.3	199.3	199.3	199.3	199.3	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	24.1	24.1	24.1	18.0	18.0	48.4	37.4
Battery24	57.1	57.1	53.8	53.8	53.8	40.3	40.3	29.9	29.9	29.9	22.4	22.4	0.0	0.0
Civil	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
CoreNational	7.9	0.0	0.0	7.9	0.0	7.9	0.0	0.0	7.9	0.0	7.9	0.0	0.0	0.0
CoreState	0.0	44.5	0.0	0.0	44.5	0.0	44.5	0.0	0.0	44.5	0.0	44.5	0.0	0.0
PreferentialAccess	4.0	31.8	4.0	7.9	35.8	11.9	39.7	4.0	7.9	35.8	11.9	39.7	4.0	0.0
LMRIntegration	15.9	127.1	15.9	31.8	143.0	47.7	158.9	15.9	31.8	143.0	47.7	158.9	15.9	31.8
OSSBSS	39.7	317.8	0.0	39.7	317.8	39.7	317.8	0.0	39.7	317.8	39.7	317.8	0.0	0.0
Handset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
RuggedisedHandset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
IVModem	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Spectrum	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	16.7	16.7	16.7	16.7	16.7	16.7	16.7	16.7	16.7	16.7	80.3	80.3
CoreNetworkAugmentation	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3
BackhaulUrban	681.7	681.7	425.9	608.4	608.4	608.4	608.4	465.0	664.2	664.2	664.2	664.2	456.8	137.0
BackhaulRegional	732.8	732.8	512.9	732.8	732.8	732.8	732.8	561.4	561.4	561.4	561.4	561.4	611.5	474.7
SiteLeasingUrban	647.6	647.6	578.0	578.0	578.0	578.0	578.0	631.0	631.0	631.0	631.0	631.0	0.0	0.0
SiteLeasingRegional	348.1	348.1	348.1	348.1	348.1	348.1	348.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Total operating costs	2 987.8	3 441.4	2 382.1	2 852.0	3 305.7	2 858.4	3 312.1	1 985.8	2 252.6	2 706.3	2 259.0	2 712.7	1 218.2	762.5

[a] National approach. [b] State-by-state approach.

Table C.32 Net present value of costs (lower bound opportunity cost of spectrum)

$ millions

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Total costs														
Total	5 991.0	7 407.2	4 940.7	5 643.1	7 059.3	5 652.9	7 069.1	4 223.7	4 729.5	6 145.7	4 738.0	6 154.3	2 083.0	2 107.2
Capital Expenditure														
NewSiteBuildMetro	70.7	70.7	60.8	60.8	60.8	60.8	60.8	65.9	65.9	65.9	65.9	65.9	0.0	0.0
NewSiteBuildRegional	39.9	39.9	39.9	39.9	39.9	39.9	39.9	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	1 039.3	1 039.3	947.1	947.1	947.1	947.1	947.1	626.0	626.0	626.0	626.0	626.0	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	51.6	51.6	51.6	38.7	38.7	103.0	77.3
Battery24	155.9	155.9	142.1	142.1	142.1	106.6	106.6	93.9	93.9	93.9	70.4	70.4	0.0	0.0
Civil	18.4	18.4	16.8	16.8	16.8	16.8	16.8	18.2	18.2	18.2	18.2	18.2	14.3	14.3
CoreNational	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	0.0
CoreState	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0
PreferentialAccess	8.4	67.4	8.4	16.9	75.9	25.3	84.3	8.4	16.9	75.9	25.3	84.3	8.4	16.9
LMRIntegration	33.7	269.7	33.7	67.4	303.4	101.1	337.1	33.7	67.4	303.4	101.1	337.1	33.7	67.4
OSSBSS	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	0.0
Handset	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2
RuggedisedHandset	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5
IVModem	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1
Spectrum	131.8	131.8	131.8	131.8	131.8	131.8	131.8	112.0	112.0	112.0	112.0	112.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	170.6	170.6
CoreNetworkAugmentation	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8
Total capital expenditure	2 133.9	3 096.4	1 950.7	2 094.0	3 056.5	2 100.6	3 063.2	1 579.9	1 723.2	2 685.7	1 729.0	2 691.5	864.8	881.2

[a] National approach. [b] State-by-state approach.

(continued next page)

Table C.32 (continued)

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Operating costs														
NewSiteBuildMetro	59.0	59.0	50.7	50.7	50.7	50.7	50.7	55.3	55.3	55.3	55.3	55.3	0.0	0.0
NewSiteBuildRegional	33.2	33.2	33.2	33.2	33.2	33.2	33.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	491.3	491.3	447.4	447.4	447.4	447.4	447.4	295.0	295.0	295.0	295.0	295.0	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	24.2	24.2	24.2	18.2	18.2	48.4	36.3
Battery24	73.7	73.7	67.1	67.1	67.1	50.3	50.3	44.2	44.2	44.2	33.2	33.2	0.0	0.0
Civil	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
CoreNational	7.9	0.0	0.0	7.9	0.0	7.9	0.0	0.0	7.9	0.0	7.9	0.0	0.0	0.0
CoreState	0.0	44.5	0.0	0.0	44.5	0.0	44.5	0.0	0.0	44.5	0.0	44.5	0.0	0.0
PreferentialAccess	4.0	31.8	4.0	7.9	35.8	11.9	39.7	4.0	7.9	35.8	11.9	39.7	4.0	7.9
LMRIntegration	15.9	127.1	15.9	31.8	143.0	47.7	158.9	15.9	31.8	143.0	47.7	158.9	15.9	31.8
OSSBSS	39.7	317.8	0.0	39.7	317.8	39.7	317.8	0.0	39.7	317.8	39.7	317.8	0.0	0.0
Handset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
RuggedisedHandset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
IVModem	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Spectrum	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	16.7	16.7	16.7	16.7	16.7	16.7	16.7	16.7	16.7	16.7	80.3	80.3
CoreNetworkAugmentation	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3
BackhaulUrban	1 048.1	1 048.1	631.1	901.5	901.5	901.5	901.5	688.3	983.3	983.3	983.3	983.3	456.8	456.8
BackhaulRegional	737.2	737.2	516.0	737.2	737.2	737.2	737.2	564.8	564.8	564.8	564.8	564.8	611.5	611.5
SiteLeasingUrban	995.7	995.7	856.5	856.5	856.5	856.5	856.5	934.1	934.1	934.1	934.1	934.1	0.0	0.0
SiteLeasingRegional	350.2	350.2	350.2	350.2	350.2	350.2	350.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Total operating costs	3 857.1	4 310.8	2 990.0	3 549.1	4 002.8	3 552.2	4 005.9	2 643.8	3 006.3	3 460.0	3 009.1	3 462.8	1 218.2	1 226.0

[a] National approach. [b] State-by-state approach.

Table C.33 **Net present value of costs (upper bound opportunity cost of spectrum)**

$ millions

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Total costs														
Total	6 212.4	7 628.6	5 162.1	5 864.5	7 280.7	5 874.2	7 290.5	4 411.9	4 917.7	6 333.9	4 926.2	6 342.4	2 083.0	2 107.2
Capital Expenditure														
NewSiteBuildMetro	70.7	70.7	60.8	60.8	60.8	60.8	60.8	65.9	65.9	65.9	65.9	65.9	0.0	0.0
NewSiteBuildRegional	39.9	39.9	39.9	39.9	39.9	39.9	39.9	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	1 039.3	1 039.3	947.1	947.1	947.1	947.1	947.1	626.0	626.0	626.0	626.0	626.0	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	51.6	51.6	51.6	38.7	38.7	103.0	77.3
Battery24	155.9	155.9	142.1	142.1	142.1	106.6	106.6	93.9	93.9	93.9	70.4	70.4	0.0	0.0
Civil	18.4	18.4	16.8	16.8	16.8	16.8	16.8	18.2	18.2	18.2	18.2	18.2	14.3	14.3
CoreNational	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	0.0
CoreState	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0
PreferentialAccess	8.4	67.4	8.4	16.9	75.9	25.3	84.3	8.4	16.9	75.9	25.3	84.3	8.4	16.9
LMRIntegration	33.7	269.7	33.7	67.4	303.4	101.1	337.1	33.7	67.4	303.4	101.1	337.1	33.7	67.4
OSSBSS	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	0.0
Handset	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2
RuggedisedHandset	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5
IVModem	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1
Spectrum	353.2	353.2	353.2	353.2	353.2	353.2	353.2	300.2	300.2	300.2	300.2	300.2	0.0	0.0
MNOSitesAugmentation	0.0	0.0	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	170.6	170.6
CoreNetworkAugmentation	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8
Total capital expenditure	2 355.3	3 317.8	2 172.1	2 315.4	3 277.9	2 322.0	3 284.5	1 768.1	1 911.4	2 873.9	1 917.2	2 879.7	864.8	881.2

[a] National approach. [b] State-by-state approach.

(continued next page)

Table C.33 (continued)

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Operating costs														
NewSiteBuildMetro	59.0	59.0	50.7	50.7	50.7	50.7	50.7	55.3	55.3	55.3	55.3	55.3	0.0	0.0
NewSiteBuildRegional	33.2	33.2	33.2	33.2	33.2	33.2	33.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	491.3	491.3	447.4	447.4	447.4	447.4	447.4	295.0	295.0	295.0	295.0	295.0	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	24.2	24.2	24.2	18.2	18.2	48.4	36.3
Battery24	73.7	73.7	67.1	67.1	67.1	50.3	50.3	44.2	44.2	44.2	33.2	33.2	0.0	0.0
Civil	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
CoreNational	7.9	0.0	0.0	7.9	0.0	7.9	0.0	0.0	7.9	0.0	7.9	0.0	0.0	0.0
CoreState	0.0	44.5	0.0	0.0	44.5	0.0	44.5	0.0	0.0	44.5	0.0	44.5	0.0	0.0
PreferentialAccess	4.0	31.8	4.0	7.9	35.8	11.9	39.7	4.0	7.9	35.8	11.9	39.7	4.0	7.9
LMRIntegration	15.9	127.1	15.9	31.8	143.0	47.7	158.9	15.9	31.8	143.0	47.7	158.9	15.9	31.8
OSSBSS	39.7	317.8	0.0	39.7	317.8	39.7	317.8	0.0	39.7	317.8	39.7	317.8	0.0	0.0
Handset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
RuggedisedHandset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
IVModem	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Spectrum	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	16.7	16.7	16.7	16.7	16.7	16.7	16.7	16.7	16.7	16.7	80.3	80.3
CoreNetworkAugmentation	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3
BackhaulUrban	1 048.1	1 048.1	631.1	901.5	901.5	901.5	901.5	688.3	983.3	983.3	983.3	983.3	456.8	456.8
BackhaulRegional	737.2	737.2	516.0	737.2	737.2	737.2	737.2	564.8	564.8	564.8	564.8	564.8	611.5	611.5
SiteLeasingUrban	995.7	995.7	856.5	856.5	856.5	856.5	856.5	934.1	934.1	934.1	934.1	934.1	0.0	0.0
SiteLeasingRegional	350.2	350.2	350.2	350.2	350.2	350.2	350.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Total operating costs	3 857.1	4 310.8	2 990.0	3 549.1	4 002.8	3 552.2	4 005.9	2 643.8	3 006.3	3 460.0	3 009.1	3 462.8	1 218.2	1 226.0

[a] National approach. [b] State-by-state approach.

Table C.34 **Net present value of costs (lower bound site equipment cost)**
$ millions

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Total costs														
Total	5 548.8	6 965.0	4 530.0	5 232.4	6 648.6	5 242.1	6 658.3	3 970.8	4 476.6	5 892.8	4 485.1	5 901.3	1 988.9	2 013.1
Capital Expenditure														
NewSiteBuildMetro	70.7	70.7	60.8	60.8	60.8	60.8	60.8	65.9	65.9	65.9	65.9	65.9	0.0	0.0
NewSiteBuildRegional	39.9	39.9	39.9	39.9	39.9	39.9	39.9	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	649.6	649.6	591.9	591.9	591.9	591.9	591.9	391.3	391.3	391.3	391.3	391.3	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	51.6	51.6	51.6	38.7	38.7	103.0	77.3
Battery24	155.9	155.9	142.1	142.1	142.1	106.6	106.6	93.9	93.9	93.9	70.4	70.4	0.0	0.0
Civil	18.4	18.4	16.8	16.8	16.8	16.8	16.8	18.2	18.2	18.2	18.2	18.2	14.3	14.3
CoreNational	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	0.0
CoreState	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0
PreferentialAccess	8.4	67.4	8.4	16.9	75.9	25.3	84.3	8.4	16.9	75.9	25.3	84.3	8.4	16.9
LMRIntegration	33.7	269.7	33.7	67.4	303.4	101.1	337.1	33.7	67.4	303.4	101.1	337.1	33.7	67.4
OSSBSS	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	0.0
Handset	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2
RuggedisedHandset	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5
IVModem	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1
Spectrum	263.6	263.6	263.6	263.6	263.6	263.6	263.6	224.0	224.0	224.0	224.0	224.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	22.2	22.2	22.2	22.2	22.2	22.2	22.2	22.2	22.2	22.2	106.6	106.6
CoreNetworkAugmentation	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8
Total capital expenditure	1 876.0	2 838.5	1 714.0	1 857.3	2 819.8	1 863.9	2 826.5	1 443.9	1 587.2	2 549.7	1 592.9	2 555.4	800.8	817.2

[a] National approach. [b] State-by-state approach.

(continued next page)

Table C.34 (continued)

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Operating costs														
NewSiteBuildMetro	59.0	59.0	50.7	50.7	50.7	50.7	50.7	55.3	55.3	55.3	55.3	55.3	0.0	0.0
NewSiteBuildRegional	33.2	33.2	33.2	33.2	33.2	33.2	33.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	307.1	307.1	279.6	279.6	279.6	279.6	279.6	184.4	184.4	184.4	184.4	184.4	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	24.2	24.2	24.2	18.2	18.2	48.4	36.3
Battery24	73.7	73.7	67.1	67.1	67.1	50.3	50.3	44.2	44.2	44.2	33.2	33.2	0.0	0.0
Civil	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
CoreNational	7.9	0.0	0.0	7.9	0.0	7.9	0.0	0.0	7.9	0.0	7.9	0.0	0.0	0.0
CoreState	0.0	44.5	0.0	0.0	44.5	0.0	44.5	0.0	0.0	44.5	0.0	44.5	0.0	0.0
PreferentialAccess	4.0	31.8	4.0	7.9	35.8	11.9	39.7	4.0	7.9	35.8	11.9	39.7	4.0	7.9
LMRIntegration	15.9	127.1	15.9	31.8	143.0	47.7	158.9	15.9	31.8	143.0	47.7	158.9	15.9	31.8
OSSBSS	39.7	317.8	0.0	39.7	317.8	39.7	317.8	0.0	39.7	317.8	39.7	317.8	0.0	0.0
Handset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
RuggedisedHandset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
IVModem	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Spectrum	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	10.4	10.4	10.4	10.4	10.4	10.4	10.4	10.4	10.4	10.4	50.2	50.2
CoreNetworkAugmentation	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3
BackhaulUrban	1 048.1	1 048.1	631.1	901.5	901.5	901.5	901.5	688.3	983.3	983.3	983.3	983.3	456.8	456.8
BackhaulRegional	737.2	737.2	516.0	737.2	737.2	737.2	737.2	564.8	564.8	564.8	564.8	564.8	611.5	611.5
SiteLeasingUrban	995.7	995.7	856.5	856.5	856.5	856.5	856.5	934.1	934.1	934.1	934.1	934.1	0.0	0.0
SiteLeasingRegional	350.2	350.2	350.2	350.2	350.2	350.2	350.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Total operating costs	3 672.8	4 126.5	2 815.9	3 375.1	3 828.8	3 378.2	3 831.9	2 526.9	2 889.4	3 343.1	2 892.2	3 345.9	1 188.1	1 195.9

[a] National approach. [b] State-by-state approach.

Table C.35 **Net present value of costs (upper bound site equipment cost)**
$ millions

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Total costs														
Total	6 888.1	8 304.3	5 795.8	6 498.3	7 914.5	6 508.0	7 924.2	4 822.3	5 328.1	6 744.3	5 336.6	6 752.9	2 208.5	2 232.6
Capital Expenditure														
NewSiteBuildMetro	70.7	70.7	60.8	60.8	60.8	60.8	60.8	65.9	65.9	65.9	65.9	65.9	0.0	0.0
NewSiteBuildRegional	39.9	39.9	39.9	39.9	39.9	39.9	39.9	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	1 558.9	1 558.9	1 420.7	1 420.7	1 420.7	1 420.7	1 420.7	939.0	939.0	939.0	939.0	939.0	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	51.6	51.6	51.6	38.7	38.7	103.0	77.3
Battery24	155.9	155.9	142.1	142.1	142.1	106.6	106.6	93.9	93.9	93.9	70.4	70.4	0.0	0.0
Civil	18.4	18.4	16.8	16.8	16.8	16.8	16.8	18.2	18.2	18.2	18.2	18.2	14.3	14.3
CoreNational	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	0.0
CoreState	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0
PreferentialAccess	8.4	67.4	8.4	16.9	75.9	25.3	84.3	8.4	16.9	75.9	25.3	84.3	8.4	16.9
LMRIntegration	33.7	269.7	33.7	67.4	303.4	101.1	337.1	33.7	67.4	303.4	101.1	337.1	33.7	67.4
OSSBSS	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	0.0
Handset	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2
RuggedisedHandset	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5
IVModem	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1
Spectrum	263.6	263.6	263.6	263.6	263.6	263.6	263.6	224.0	224.0	224.0	224.0	224.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	53.2	53.2	53.2	53.2	53.2	53.2	53.2	53.2	53.2	53.2	255.9	255.9
CoreNetworkAugmentation	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8
Total capital expenditure	2 785.4	3 747.9	2 573.8	2 717.1	3 679.6	2 723.7	3 686.2	2 022.7	2 166.0	3 128.5	2 171.7	3 134.2	950.1	966.5

[a] National approach. [b] State-by-state approach.

(continued next page)

Table C.35 (continued)

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Operating costs														
NewSiteBuildMetro	59.0	59.0	50.7	50.7	50.7	50.7	50.7	55.3	55.3	55.3	55.3	55.3	0.0	0.0
NewSiteBuildRegional	33.2	33.2	33.2	33.2	33.2	33.2	33.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	737.0	737.0	671.1	671.1	671.1	671.1	671.1	442.5	442.5	442.5	442.5	442.5	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	24.2	24.2	24.2	18.2	18.2	48.4	36.3
Battery24	73.7	73.7	67.1	67.1	67.1	50.3	50.3	44.2	44.2	44.2	33.2	33.2	0.0	0.0
Civil	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
CoreNational	7.9	0.0	0.0	7.9	0.0	7.9	0.0	0.0	7.9	0.0	7.9	0.0	0.0	0.0
CoreState	0.0	44.5	0.0	0.0	44.5	0.0	44.5	0.0	0.0	44.5	0.0	44.5	0.0	0.0
PreferentialAccess	4.0	31.8	4.0	7.9	35.8	11.9	39.7	4.0	7.9	35.8	11.9	39.7	4.0	7.9
LMRIntegration	15.9	127.1	15.9	31.8	143.0	47.7	158.9	15.9	31.8	143.0	47.7	158.9	15.9	31.8
OSSBSS	39.7	317.8	0.0	39.7	317.8	39.7	317.8	0.0	39.7	317.8	39.7	317.8	0.0	0.0
Handset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
RuggedisedHandset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
IVModem	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Spectrum	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	25.0	25.0	25.0	25.0	25.0	25.0	25.0	25.0	25.0	25.0	120.4	120.4
CoreNetworkAugmentation	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3
BackhaulUrban	1 048.1	1 048.1	631.1	901.5	901.5	901.5	901.5	688.3	983.3	983.3	983.3	983.3	456.8	456.8
BackhaulRegional	737.2	737.2	516.0	737.2	737.2	737.2	737.2	564.8	564.8	564.8	564.8	564.8	611.5	611.5
SiteLeasingUrban	995.7	995.7	856.5	856.5	856.5	856.5	856.5	934.1	934.1	934.1	934.1	934.1	0.0	0.0
SiteLeasingRegional	350.2	350.2	350.2	350.2	350.2	350.2	350.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Total operating costs	4 102.7	4 556.4	3 222.0	3 781.2	4 234.9	3 784.3	4 237.9	2 799.6	3 162.2	3 615.9	3 164.9	3 618.6	1 258.4	1 266.1

[a] National approach. [b] State-by-state approach.

Table C.36 **Net present value of costs (lower bound number of greenfield sites)**

$ millions

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Total costs														
Total	5 990.9	7 407.1	4 951.4	5 653.8	7 070.1	5 663.6	7 079.8	4 263.7	4 769.5	6 185.7	4 778.0	6 194.2	2 083.0	2 107.2
Capital Expenditure														
NewSiteBuildMetro	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
NewSiteBuildRegional	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	1 039.3	1 039.3	947.1	947.1	947.1	947.1	947.1	626.0	626.0	626.0	626.0	626.0	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	51.6	51.6	51.6	38.7	38.7	103.0	77.3
Battery24	155.9	155.9	142.1	142.1	142.1	106.6	106.6	93.9	93.9	93.9	70.4	70.4	0.0	0.0
Civil	18.4	18.4	16.8	16.8	16.8	16.8	16.8	18.2	18.2	18.2	18.2	18.2	14.3	14.3
CoreNational	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	0.0
CoreState	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0
PreferentialAccess	8.4	67.4	8.4	16.9	75.9	25.3	84.3	8.4	16.9	75.9	25.3	84.3	8.4	16.9
LMRIntegration	33.7	269.7	33.7	67.4	303.4	101.1	337.1	33.7	67.4	303.4	101.1	337.1	33.7	67.4
OSSBSS	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	0.0
Handset	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2
RuggedisedHandset	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5
IVModem	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1
Spectrum	263.6	263.6	263.6	263.6	263.6	263.6	263.6	224.0	224.0	224.0	224.0	224.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	170.6	170.6
CoreNetworkAugmentation	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8
Total capital expenditure	2 155.1	3 117.7	1 981.8	2 125.1	3 087.6	2 131.7	3 094.2	1 626.0	1 769.3	2 731.8	1 775.1	2 737.6	864.8	881.2

[a] National approach. [b] State-by-state approach.

(continued next page)

Table C.36 (continued)

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Operating costs														
NewSiteBuildMetro	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
NewSiteBuildRegional	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	491.3	491.3	447.4	447.4	447.4	447.4	447.4	295.0	295.0	295.0	295.0	295.0	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	24.2	24.2	24.2	18.2	18.2	48.4	36.3
Battery24	73.7	73.7	67.1	67.1	67.1	50.3	50.3	44.2	44.2	44.2	33.2	33.2	0.0	0.0
Civil	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
CoreNational	7.9	0.0	0.0	7.9	0.0	7.9	0.0	0.0	7.9	0.0	7.9	0.0	0.0	0.0
CoreState	0.0	44.5	0.0	0.0	44.5	0.0	44.5	0.0	0.0	44.5	0.0	44.5	0.0	0.0
PreferentialAccess	4.0	31.8	4.0	7.9	35.8	11.9	39.7	4.0	7.9	35.8	11.9	39.7	4.0	7.9
LMRIntegration	15.9	127.1	15.9	31.8	143.0	47.7	158.9	15.9	31.8	143.0	47.7	158.9	15.9	31.8
OSSBSS	39.7	317.8	0.0	39.7	317.8	39.7	317.8	0.0	39.7	317.8	39.7	317.8	0.0	0.0
Handset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
RuggedisedHandset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
IVModem	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Spectrum	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	16.7	16.7	16.7	16.7	16.7	16.7	16.7	16.7	16.7	16.7	80.3	80.3
CoreNetworkAugmentation	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3
BackhaulUrban	1 048.1	1 048.1	631.1	901.5	901.5	901.5	901.5	688.3	983.3	983.3	983.3	983.3	456.8	456.8
BackhaulRegional	737.2	737.2	516.0	737.2	737.2	737.2	737.2	564.8	564.8	564.8	564.8	564.8	611.5	611.5
SiteLeasingUrban	1 048.1	1 048.1	901.5	901.5	901.5	901.5	901.5	983.3	983.3	983.3	983.3	983.3	0.0	0.0
SiteLeasingRegional	368.6	368.6	368.6	368.6	368.6	368.6	368.6	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Total operating costs	3 835.8	4 289.5	2 969.6	3 528.8	3 982.4	3 531.8	3 985.5	2 637.7	3 000.2	3 453.9	3 002.9	3 456.6	1 218.2	1 226.0

[a] National approach. [b] State-by-state approach.

Table C.37 **Net present value of costs (upper bound number of greenfield sites)**

$ millions

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Total costs														
Total	6 386.5	7 802.7	5 314.6	6 017.1	7 433.3	6 026.8	7 443.0	4 479.9	4 985.7	6 401.9	4 994.2	6 410.4	2 083.0	2 107.2
Capital Expenditure														
NewSiteBuildMetro	212.0	212.0	182.4	182.4	182.4	182.4	182.4	197.8	197.8	197.8	197.8	197.8	0.0	0.0
NewSiteBuildRegional	119.6	119.6	119.6	119.6	119.6	119.6	119.6	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	1 039.3	1 039.3	947.1	947.1	947.1	947.1	947.1	626.0	626.0	626.0	626.0	626.0	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	51.6	51.6	51.6	38.7	38.7	103.0	77.3
Battery24	155.9	155.9	142.1	142.1	142.1	106.6	106.6	93.9	93.9	93.9	70.4	70.4	0.0	0.0
Civil	18.4	18.4	16.8	16.8	16.8	16.8	16.8	18.2	18.2	18.2	18.2	18.2	14.3	14.3
CoreNational	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	0.0
CoreState	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0
PreferentialAccess	8.4	67.4	8.4	16.9	75.9	25.3	84.3	8.4	16.9	75.9	25.3	84.3	8.4	16.9
LMRIntegration	33.7	269.7	33.7	67.4	303.4	101.1	337.1	33.7	67.4	303.4	101.1	337.1	33.7	67.4
OSSBSS	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	0.0
Handset	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2
RuggedisedHandset	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5
IVModem	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1
Spectrum	263.6	263.6	263.6	263.6	263.6	263.6	263.6	224.0	224.0	224.0	224.0	224.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	170.6	170.6
CoreNetworkAugmentation	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8
Total capital expenditure	2 486.8	3 449.3	2 283.9	2 427.2	3 389.7	2 433.8	3 396.3	1 823.8	1 967.1	2 929.6	1 972.8	2 935.3	864.8	881.2

[a] National approach. [b] State-by-state approach.

(continued next page)

Table C.37 (continued)

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Operating costs														
NewSiteBuildMetro	176.9	176.9	152.1	152.1	152.1	152.1	152.1	165.9	165.9	165.9	165.9	165.9	0.0	0.0
NewSiteBuildRegional	99.5	99.5	99.5	99.5	99.5	99.5	99.5	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	491.3	491.3	447.4	447.4	447.4	447.4	447.4	295.0	295.0	295.0	295.0	295.0	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	24.2	24.2	24.2	18.2	18.2	48.4	36.3
Battery24	73.7	73.7	67.1	67.1	67.1	50.3	50.3	44.2	44.2	44.2	33.2	33.2	0.0	0.0
Civil	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
CoreNational	7.9	0.0	0.0	7.9	0.0	7.9	0.0	0.0	7.9	0.0	7.9	0.0	0.0	0.0
CoreState	0.0	44.5	0.0	0.0	44.5	0.0	44.5	0.0	0.0	44.5	0.0	44.5	0.0	0.0
PreferentialAccess	4.0	31.8	4.0	7.9	35.8	11.9	39.7	4.0	7.9	35.8	11.9	39.7	4.0	7.9
LMRIntegration	15.9	127.1	15.9	31.8	143.0	47.7	158.9	15.9	31.8	143.0	47.7	158.9	15.9	31.8
OSSBSS	39.7	317.8	0.0	39.7	317.8	39.7	317.8	0.0	39.7	317.8	39.7	317.8	0.0	0.0
Handset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
RuggedisedHandset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
IVModem	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Spectrum	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	16.7	16.7	16.7	16.7	16.7	16.7	16.7	16.7	16.7	16.7	80.3	80.3
CoreNetworkAugmentation	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3
BackhaulUrban	1 048.1	1 048.1	631.1	901.5	901.5	901.5	901.5	688.3	983.3	983.3	983.3	983.3	456.8	456.8
BackhaulRegional	737.2	737.2	516.0	737.2	737.2	737.2	737.2	564.8	564.8	564.8	564.8	564.8	611.5	611.5
SiteLeasingUrban	890.8	890.8	766.3	766.3	766.3	766.3	766.3	835.8	835.8	835.8	835.8	835.8	0.0	0.0
SiteLeasingRegional	313.3	313.3	313.3	313.3	313.3	313.3	313.3	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Total operating costs	3 899.7	4 353.3	3 030.7	3 589.9	4 043.6	3 593.0	4 046.7	2 656.1	3 018.6	3 472.3	3 021.4	3 475.1	1 218.2	1 226.0

[a] National approach. [b] State-by-state approach.

Table C.38 **Net present value of costs (lower bound cost of greenfield site build)**
$ millions

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Total costs														
Total	6 021.4	7 437.6	4 980.2	5 682.6	7 098.8	5 692.3	7 108.6	4 275.1	4 780.9	6 197.1	4 789.5	6 205.7	2 083.0	2 107.2
Capital Expenditure														
NewSiteBuildMetro	35.3	35.3	30.4	30.4	30.4	30.4	30.4	33.0	33.0	33.0	33.0	33.0	0.0	0.0
NewSiteBuildRegional	19.9	19.9	19.9	19.9	19.9	19.9	19.9	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	1 039.3	1 039.3	947.1	947.1	947.1	947.1	947.1	626.0	626.0	626.0	626.0	626.0	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	51.6	51.6	51.6	38.7	38.7	103.0	77.3
Battery24	155.9	155.9	142.1	142.1	142.1	106.6	106.6	93.9	93.9	93.9	70.4	70.4	0.0	0.0
Civil	18.4	18.4	16.8	16.8	16.8	16.8	16.8	18.2	18.2	18.2	18.2	18.2	14.3	14.3
CoreNational	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	0.0
CoreState	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0
PreferentialAccess	8.4	67.4	8.4	16.9	75.9	25.3	84.3	8.4	16.9	75.9	25.3	84.3	8.4	16.9
LMRIntegration	33.7	269.7	33.7	67.4	303.4	101.1	337.1	33.7	67.4	303.4	101.1	337.1	33.7	67.4
OSSBSS	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	0.0
Handset	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2
RuggedisedHandset	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5
IVModem	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1
Spectrum	263.6	263.6	263.6	263.6	263.6	263.6	263.6	224.0	224.0	224.0	224.0	224.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	170.6	170.6
CoreNetworkAugmentation	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8
Total capital expenditure	2 210.4	3 172.9	2 032.2	2 175.4	3 138.0	2 182.1	3 144.6	1 659.0	1 802.3	2 764.8	1 808.0	2 770.5	864.8	881.2

[a] National approach. [b] State-by-state approach.

(continued next page)

Table C.38 (continued)

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Operating costs														
NewSiteBuildMetro	29.5	29.5	25.4	25.4	25.4	25.4	25.4	27.7	27.7	27.7	27.7	27.7	0.0	0.0
NewSiteBuildRegional	16.6	16.6	16.6	16.6	16.6	16.6	16.6	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	491.3	491.3	447.4	447.4	447.4	447.4	447.4	295.0	295.0	295.0	295.0	295.0	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	24.2	24.2	24.2	18.2	18.2	48.4	36.3
Battery24	73.7	73.7	67.1	67.1	67.1	50.3	50.3	44.2	44.2	44.2	33.2	33.2	0.0	0.0
Civil	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
CoreNational	7.9	0.0	0.0	7.9	0.0	7.9	0.0	0.0	7.9	0.0	7.9	0.0	0.0	0.0
CoreState	0.0	44.5	0.0	0.0	44.5	0.0	44.5	0.0	0.0	44.5	0.0	44.5	0.0	0.0
PreferentialAccess	4.0	31.8	4.0	7.9	35.8	11.9	39.7	4.0	7.9	35.8	11.9	39.7	4.0	7.9
LMRIntegration	15.9	127.1	15.9	31.8	143.0	47.7	158.9	15.9	31.8	143.0	47.7	158.9	15.9	31.8
OSSBSS	39.7	317.8	0.0	39.7	317.8	39.7	317.8	0.0	39.7	317.8	39.7	317.8	0.0	0.0
Handset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
RuggedisedHandset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
IVModem	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Spectrum	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	16.7	16.7	16.7	16.7	16.7	16.7	16.7	16.7	16.7	16.7	80.3	80.3
CoreNetworkAugmentation	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3
BackhaulUrban	1 048.1	1 048.1	631.1	901.5	901.5	901.5	901.5	688.3	983.3	983.3	983.3	983.3	456.8	456.8
BackhaulRegional	737.2	737.2	516.0	737.2	737.2	737.2	737.2	564.8	564.8	564.8	564.8	564.8	611.5	611.5
SiteLeasingUrban	995.7	995.7	856.5	856.5	856.5	856.5	856.5	934.1	934.1	934.1	934.1	934.1	0.0	0.0
SiteLeasingRegional	350.2	350.2	350.2	350.2	350.2	350.2	350.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Total operating costs	3 811.0	4 264.7	2 948.0	3 507.2	3 960.9	3 510.3	3 964.0	2 616.2	2 978.7	3 432.4	2 981.4	3 435.1	1 218.2	1 226.0

[a] National approach. [b] State-by-state approach.

Table C.39 **Net present value of costs (upper bound cost of greenfield site build)**
$ millions

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Total costs														
Total	6 224.1	7 640.3	5 164.8	5 867.2	7 283.4	5 876.9	7 293.1	4 396.4	4 902.2	6 318.4	4 910.7	6 326.9	2 083.0	2 107.2
Capital Expenditure														
NewSiteBuildMetro	106.0	106.0	91.2	91.2	91.2	91.2	91.2	98.9	98.9	98.9	98.9	98.9	0.0	0.0
NewSiteBuildRegional	59.8	59.8	59.8	59.8	59.8	59.8	59.8	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	1 039.3	1 039.3	947.1	947.1	947.1	947.1	947.1	626.0	626.0	626.0	626.0	626.0	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	51.6	51.6	51.6	38.7	38.7	103.0	77.3
Battery24	155.9	155.9	142.1	142.1	142.1	106.6	106.6	93.9	93.9	93.9	70.4	70.4	0.0	0.0
Civil	18.4	18.4	16.8	16.8	16.8	16.8	16.8	18.2	18.2	18.2	18.2	18.2	14.3	14.3
CoreNational	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	0.0
CoreState	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0
PreferentialAccess	8.4	67.4	8.4	16.9	75.9	25.3	84.3	8.4	16.9	75.9	25.3	84.3	8.4	16.9
LMRIntegration	33.7	269.7	33.7	67.4	303.4	101.1	337.1	33.7	67.4	303.4	101.1	337.1	33.7	67.4
OSSBSS	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	0.0
Handset	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2
RuggedisedHandset	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5
IVModem	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1
Spectrum	263.6	263.6	263.6	263.6	263.6	263.6	263.6	224.0	224.0	224.0	224.0	224.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	170.6	170.6
CoreNetworkAugmentation	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8
Total capital expenditure	2 321.0	3 283.5	2 132.9	2 276.1	3 238.7	2 282.8	3 245.3	1 724.9	1 868.2	2 830.7	1 873.9	2 836.5	864.8	881.2

[a] National approach. [b] State-by-state approach.

(continued next page)

Table C.39 (continued)

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Operating costs														
NewSiteBuildMetro	88.4	88.4	76.1	76.1	76.1	76.1	76.1	83.0	83.0	83.0	83.0	83.0	0.0	0.0
NewSiteBuildRegional	49.8	49.8	49.8	49.8	49.8	49.8	49.8	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	491.3	491.3	447.4	447.4	447.4	447.4	447.4	295.0	295.0	295.0	295.0	295.0	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	24.2	24.2	24.2	18.2	18.2	48.4	36.3
Battery24	73.7	73.7	67.1	67.1	67.1	50.3	50.3	44.2	44.2	44.2	33.2	33.2	0.0	0.0
Civil	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
CoreNational	7.9	0.0	0.0	7.9	0.0	7.9	0.0	0.0	7.9	0.0	7.9	0.0	0.0	0.0
CoreState	0.0	44.5	0.0	0.0	44.5	0.0	44.5	0.0	0.0	44.5	0.0	44.5	0.0	0.0
PreferentialAccess	4.0	31.8	4.0	7.9	35.8	11.9	39.7	4.0	7.9	35.8	11.9	39.7	4.0	7.9
LMRIntegration	15.9	127.1	15.9	31.8	143.0	47.7	158.9	15.9	31.8	143.0	47.7	158.9	15.9	31.8
OSSBSS	39.7	317.8	0.0	39.7	317.8	39.7	317.8	0.0	39.7	317.8	39.7	317.8	0.0	0.0
Handset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
RuggedisedHandset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
IVModem	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Spectrum	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	16.7	16.7	16.7	16.7	16.7	16.7	16.7	16.7	16.7	16.7	80.3	80.3
CoreNetworkAugmentation	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3
BackhaulUrban	1 048.1	1 048.1	631.1	901.5	901.5	901.5	901.5	688.3	983.3	983.3	983.3	983.3	456.8	456.8
BackhaulRegional	737.2	737.2	516.0	737.2	737.2	737.2	737.2	564.8	564.8	564.8	564.8	564.8	611.5	611.5
SiteLeasingUrban	995.7	995.7	856.5	856.5	856.5	856.5	856.5	934.1	934.1	934.1	934.1	934.1	0.0	0.0
SiteLeasingRegional	350.2	350.2	350.2	350.2	350.2	350.2	350.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Total operating costs	3 903.1	4 356.8	3 031.9	3 591.1	4 044.8	3 594.2	4 047.8	2 671.5	3 034.0	3 487.7	3 036.7	3 490.4	1 218.2	1 226.0

[a] National approach. [b] State-by-state approach.

Table C.40 **Net present value of costs (lower bound network operating costs)**

$ millions

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Total costs														
Total	6 001.9	7 266.9	4 981.6	5 661.5	6 926.5	5 670.2	6 935.1	4 286.5	4 769.8	6 034.8	4 777.4	6 042.4	2 033.1	2 054.6
Capital Expenditure														
NewSiteBuildMetro	70.7	70.7	60.8	60.8	60.8	60.8	60.8	65.9	65.9	65.9	65.9	65.9	0.0	0.0
NewSiteBuildRegional	39.9	39.9	39.9	39.9	39.9	39.9	39.9	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	1 039.3	1 039.3	947.1	947.1	947.1	947.1	947.1	626.0	626.0	626.0	626.0	626.0	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	51.6	51.6	51.6	38.7	38.7	103.0	77.3
Battery24	155.9	155.9	142.1	142.1	142.1	106.6	106.6	93.9	93.9	93.9	70.4	70.4	0.0	0.0
Civil	18.4	18.4	16.8	16.8	16.8	16.8	16.8	18.2	18.2	18.2	18.2	18.2	14.3	14.3
CoreNational	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	0.0
CoreState	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0
PreferentialAccess	8.4	67.4	8.4	16.9	75.9	25.3	84.3	8.4	16.9	75.9	25.3	84.3	8.4	16.9
LMRIntegration	33.7	269.7	33.7	67.4	303.4	101.1	337.1	33.7	67.4	303.4	101.1	337.1	33.7	67.4
OSSBSS	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	0.0
Handset	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2
RuggedisedHandset	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5
IVModem	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1
Spectrum	263.6	263.6	263.6	263.6	263.6	263.6	263.6	224.0	224.0	224.0	224.0	224.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	170.6	170.6
CoreNetworkAugmentation	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8
Total capital expenditure	2 265.7	3 228.2	2 082.5	2 225.8	3 188.3	2 232.4	3 194.9	1 691.9	1 835.2	2 797.7	1 841.0	2 803.5	864.8	881.2

[a] National approach. [b] State-by-state approach.

(continued next page)

Table C.40 (continued)

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Operating costs														
NewSiteBuildMetro	39.3	39.3	33.8	33.8	33.8	33.8	33.8	36.9	36.9	36.9	36.9	36.9	0.0	0.0
NewSiteBuildRegional	22.1	22.1	22.1	22.1	22.1	22.1	22.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	327.6	327.6	298.3	298.3	298.3	298.3	298.3	196.7	196.7	196.7	196.7	196.7	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	16.1	16.1	16.1	12.1	12.1	32.3	24.2
Battery24	49.1	49.1	44.7	44.7	44.7	33.6	33.6	29.5	29.5	29.5	22.1	22.1	0.0	0.0
Civil	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
CoreNational	5.3	0.0	0.0	5.3	0.0	5.3	0.0	0.0	5.3	0.0	5.3	0.0	0.0	0.0
CoreState	0.0	29.7	0.0	0.0	29.7	0.0	29.7	0.0	0.0	29.7	0.0	29.7	0.0	0.0
PreferentialAccess	2.6	21.2	2.6	5.3	23.8	7.9	26.5	2.6	5.3	23.8	7.9	26.5	2.6	5.3
LMRIntegration	10.6	84.8	10.6	21.2	95.3	31.8	105.9	10.6	21.2	95.3	31.8	105.9	10.6	21.2
OSSBSS	26.5	211.9	0.0	26.5	211.9	26.5	211.9	0.0	26.5	211.9	26.5	211.9	0.0	0.0
Handset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
RuggedisedHandset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
IVModem	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Spectrum	121.2	121.2	121.2	121.2	121.2	121.2	121.2	103.0	103.0	103.0	103.0	103.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	11.1	11.1	11.1	11.1	11.1	11.1	11.1	11.1	11.1	11.1	53.5	53.5
CoreNetworkAugmentation	0.9	0.9	0.9	0.9	0.9	0.9	0.9	0.9	0.9	0.9	0.9	0.9	0.9	0.9
BackhaulUrban	1 048.1	1 048.1	631.1	901.5	901.5	901.5	901.5	688.3	983.3	983.3	983.3	983.3	456.8	456.8
BackhaulRegional	737.2	737.2	516.0	737.2	737.2	737.2	737.2	564.8	564.8	564.8	564.8	564.8	611.5	611.5
SiteLeasingUrban	995.7	995.7	856.5	856.5	856.5	856.5	856.5	934.1	934.1	934.1	934.1	934.1	0.0	0.0
SiteLeasingRegional	350.2	350.2	350.2	350.2	350.2	350.2	350.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Total operating costs	3 736.2	4 038.7	2 899.1	3 435.7	3 738.2	3 437.7	3 740.2	2 594.6	2 934.6	3 237.1	2 936.4	3 238.9	1 168.3	1 173.4

[a] National approach. [b] State-by-state approach.

Table C.41 **Net present value of costs (upper bound network operating costs)**
$ millions

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Total costs														
Total	6 607.1	8 174.5	5 526.9	6 251.8	7 819.3	6 262.6	7 830.0	4 693.9	5 222.2	6 789.7	5 231.7	6 799.1	2 133.0	2 159.7
Capital Expenditure														
NewSiteBuildMetro	70.7	70.7	60.8	60.8	60.8	60.8	60.8	65.9	65.9	65.9	65.9	65.9	0.0	0.0
NewSiteBuildRegional	39.9	39.9	39.9	39.9	39.9	39.9	39.9	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	1 039.3	1 039.3	947.1	947.1	947.1	947.1	947.1	626.0	626.0	626.0	626.0	626.0	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	51.6	51.6	51.6	38.7	38.7	103.0	77.3
Battery24	155.9	155.9	142.1	142.1	142.1	106.6	106.6	93.9	93.9	93.9	70.4	70.4	0.0	0.0
Civil	18.4	18.4	16.8	16.8	16.8	16.8	16.8	18.2	18.2	18.2	18.2	18.2	14.3	14.3
CoreNational	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	0.0
CoreState	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0
PreferentialAccess	8.4	67.4	8.4	16.9	75.9	25.3	84.3	8.4	16.9	75.9	25.3	84.3	8.4	16.9
LMRIntegration	33.7	269.7	33.7	67.4	303.4	101.1	337.1	33.7	67.4	303.4	101.1	337.1	33.7	67.4
OSSBSS	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	0.0
Handset	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2
RuggedisedHandset	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5
IVModem	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1
Spectrum	263.6	263.6	263.6	263.6	263.6	263.6	263.6	224.0	224.0	224.0	224.0	224.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	170.6	170.6
CoreNetworkAugmentation	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8
Total capital expenditure	2 265.7	3 228.2	2 082.5	2 225.8	3 188.3	2 232.4	3 194.9	1 691.9	1 835.2	2 797.7	1 841.0	2 803.5	864.8	881.2

[a] National approach. [b] State-by-state approach.

(continued next page)

Table C.41 (continued)

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Operating costs														
NewSiteBuildMetro	78.6	78.6	67.6	67.6	67.6	67.6	67.6	73.7	73.7	73.7	73.7	73.7	0.0	0.0
NewSiteBuildRegional	44.2	44.2	44.2	44.2	44.2	44.2	44.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	655.1	655.1	596.5	596.5	596.5	596.5	596.5	393.3	393.3	393.3	393.3	393.3	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	32.3	32.3	32.3	24.2	24.2	64.6	48.4
Battery24	98.3	98.3	89.5	89.5	89.5	67.1	67.1	59.0	59.0	59.0	44.2	44.2	0.0	0.0
Civil	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
CoreNational	10.6	0.0	0.0	10.6	0.0	10.6	0.0	0.0	10.6	0.0	10.6	0.0	0.0	0.0
CoreState	0.0	59.3	0.0	0.0	59.3	0.0	59.3	0.0	0.0	59.3	0.0	59.3	0.0	0.0
PreferentialAccess	5.3	42.4	5.3	10.6	47.7	15.9	53.0	5.3	10.6	47.7	15.9	53.0	5.3	10.6
LMRIntegration	21.2	169.5	21.2	42.4	190.7	63.6	211.9	21.2	42.4	190.7	63.6	211.9	21.2	42.4
OSSBSS	53.0	423.8	0.0	53.0	423.8	53.0	423.8	0.0	53.0	423.8	53.0	423.8	0.0	0.0
Handset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
RuggedisedHandset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
IVModem	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Spectrum	242.3	242.3	242.3	242.3	242.3	242.3	242.3	206.0	206.0	206.0	206.0	206.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	22.3	22.3	22.3	22.3	22.3	22.3	22.3	22.3	22.3	22.3	107.1	107.1
CoreNetworkAugmentation	1.7	1.7	1.7	1.7	1.7	1.7	1.7	1.7	1.7	1.7	1.7	1.7	1.7	1.7
BackhaulUrban	1 048.1	1 048.1	631.1	901.5	901.5	901.5	901.5	688.3	983.3	983.3	983.3	983.3	456.8	456.8
BackhaulRegional	737.2	737.2	516.0	737.2	737.2	737.2	737.2	564.8	564.8	564.8	564.8	564.8	611.5	611.5
SiteLeasingUrban	995.7	995.7	856.5	856.5	856.5	856.5	856.5	934.1	934.1	934.1	934.1	934.1	0.0	0.0
SiteLeasingRegional	350.2	350.2	350.2	350.2	350.2	350.2	350.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Total operating costs	4 341.4	4 946.3	3 444.4	4 026.0	4 631.0	4 030.2	4 635.1	3 002.0	3 387.0	3 991.9	3 390.7	3 995.6	1 268.2	1 278.5

[a] National approach. [b] State-by-state approach.

Table C.42 **Net present value of costs (lower bound site leasing costs)**
$ millions

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Total costs														
Total	5 803.8	7 220.0	4 788.3	5 490.8	6 907.0	5 500.5	6 916.7	4 102.2	4 608.0	6 024.2	4 616.5	6 032.7	2 083.0	1 604.0
Capital Expenditure														
NewSiteBuildMetro	70.7	70.7	60.8	60.8	60.8	60.8	60.8	65.9	65.9	65.9	65.9	65.9	0.0	0.0
NewSiteBuildRegional	39.9	39.9	39.9	39.9	39.9	39.9	39.9	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	1 039.3	1 039.3	947.1	947.1	947.1	947.1	947.1	626.0	626.0	626.0	626.0	626.0	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	51.6	51.6	51.6	38.7	38.7	103.0	79.4
Battery24	155.9	155.9	142.1	142.1	142.1	106.6	106.6	93.9	93.9	93.9	70.4	70.4	0.0	0.0
Civil	18.4	18.4	16.8	16.8	16.8	16.8	16.8	18.2	18.2	18.2	18.2	18.2	14.3	14.7
CoreNational	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	0.0
CoreState	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0
PreferentialAccess	8.4	67.4	8.4	16.9	75.9	25.3	84.3	8.4	16.9	75.9	25.3	84.3	8.4	0.0
LMRIntegration	33.7	269.7	33.7	67.4	303.4	101.1	337.1	33.7	67.4	303.4	101.1	337.1	33.7	67.4
OSSBSS	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	0.0
Handset	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2
RuggedisedHandset	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	304.2
IVModem	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	76.1
Spectrum	263.6	263.6	263.6	263.6	263.6	263.6	263.6	224.0	224.0	224.0	224.0	224.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	170.6	170.6
CoreNetworkAugmentation	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8
Total capital expenditure	2 265.7	3 228.2	2 082.5	2 225.8	3 188.3	2 232.4	3 194.9	1 691.9	1 835.2	2 797.7	1 841.0	2 803.5	864.8	841.4

[a] National approach. [b] State-by-state approach.

(continued next page)

Table C.42 (continued)

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Operating costs														
NewSiteBuildMetro	59.0	59.0	50.7	50.7	50.7	50.7	50.7	55.3	55.3	55.3	55.3	55.3	0.0	0.0
NewSiteBuildRegional	33.2	33.2	33.2	33.2	33.2	33.2	33.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	491.3	491.3	447.4	447.4	447.4	447.4	447.4	295.0	295.0	295.0	295.0	295.0	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	24.2	24.2	24.2	18.2	18.2	48.4	37.4
Battery24	73.7	73.7	67.1	67.1	67.1	50.3	50.3	44.2	44.2	44.2	33.2	33.2	0.0	0.0
Civil	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
CoreNational	7.9	0.0	0.0	7.9	0.0	7.9	0.0	0.0	7.9	0.0	7.9	0.0	0.0	0.0
CoreState	0.0	44.5	0.0	0.0	44.5	0.0	44.5	0.0	0.0	44.5	0.0	44.5	0.0	0.0
PreferentialAccess	4.0	31.8	4.0	7.9	35.8	11.9	39.7	4.0	7.9	35.8	11.9	39.7	4.0	0.0
LMRIntegration	15.9	127.1	15.9	31.8	143.0	47.7	158.9	15.9	31.8	143.0	47.7	158.9	15.9	31.8
OSSBSS	39.7	317.8	0.0	39.7	317.8	39.7	317.8	0.0	39.7	317.8	39.7	317.8	0.0	0.0
Handset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
RuggedisedHandset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
IVModem	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Spectrum	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	16.7	16.7	16.7	16.7	16.7	16.7	16.7	16.7	16.7	16.7	80.3	80.3
CoreNetworkAugmentation	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3
BackhaulUrban	1 048.1	1 048.1	631.1	901.5	901.5	901.5	901.5	688.3	983.3	983.3	983.3	983.3	456.8	137.0
BackhaulRegional	737.2	737.2	516.0	737.2	737.2	737.2	737.2	564.8	564.8	564.8	564.8	564.8	611.5	474.7
SiteLeasingUrban	746.7	746.7	642.3	642.3	642.3	642.3	642.3	700.6	700.6	700.6	700.6	700.6	0.0	0.0
SiteLeasingRegional	280.1	280.1	280.1	280.1	280.1	280.1	280.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Total operating costs	3 538.1	3 991.8	2 705.8	3 265.0	3 718.7	3 268.1	3 721.8	2 410.3	2 772.8	3 226.5	2 775.6	3 229.2	1 218.2	762.5

[a] National approach. [b] State-by-state approach.

Table C.43 **Net present value of costs (upper bound site leasing costs)**
$ millions

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Total costs														
Total	6 581.8	7 998.0	5 496.7	6 199.1	7 615.3	6 208.8	7 625.1	4 569.3	5 075.1	6 491.3	5 083.6	6 499.8	2 083.0	1 604.0
Capital Expenditure														
NewSiteBuildMetro	70.7	70.7	60.8	60.8	60.8	60.8	60.8	65.9	65.9	65.9	65.9	65.9	0.0	0.0
NewSiteBuildRegional	39.9	39.9	39.9	39.9	39.9	39.9	39.9	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	1 039.3	1 039.3	947.1	947.1	947.1	947.1	947.1	626.0	626.0	626.0	626.0	626.0	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	51.6	51.6	51.6	38.7	38.7	103.0	79.4
Battery24	155.9	155.9	142.1	142.1	142.1	106.6	106.6	93.9	93.9	93.9	70.4	70.4	0.0	0.0
Civil	18.4	18.4	16.8	16.8	16.8	16.8	16.8	18.2	18.2	18.2	18.2	18.2	14.3	14.7
CoreNational	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	0.0
CoreState	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0
PreferentialAccess	8.4	67.4	8.4	16.9	75.9	25.3	84.3	8.4	16.9	75.9	25.3	84.3	8.4	0.0
LMRIntegration	33.7	269.7	33.7	67.4	303.4	101.1	337.1	33.7	67.4	303.4	101.1	337.1	33.7	67.4
OSSBSS	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	0.0
Handset	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2
RuggedisedHandset	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	304.2
IVModem	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	76.1
Spectrum	263.6	263.6	263.6	263.6	263.6	263.6	263.6	224.0	224.0	224.0	224.0	224.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	170.6	170.6
CoreNetworkAugmentation	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8
Total capital expenditure	2 265.7	3 228.2	2 082.5	2 225.8	3 188.3	2 232.4	3 194.9	1 691.9	1 835.2	2 797.7	1 841.0	2 803.5	864.8	841.4

[a] National approach. [b] State-by-state approach.

(continued next page)

Table C.43 (continued)

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Operating costs														
NewSiteBuildMetro	59.0	59.0	50.7	50.7	50.7	50.7	50.7	55.3	55.3	55.3	55.3	55.3	0.0	0.0
NewSiteBuildRegional	33.2	33.2	33.2	33.2	33.2	33.2	33.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	491.3	491.3	447.4	447.4	447.4	447.4	447.4	295.0	295.0	295.0	295.0	295.0	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	24.2	24.2	24.2	18.2	18.2	48.4	37.4
Battery24	73.7	73.7	67.1	67.1	67.1	50.3	50.3	44.2	44.2	44.2	33.2	33.2	0.0	0.0
Civil	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
CoreNational	7.9	0.0	0.0	7.9	0.0	7.9	0.0	0.0	7.9	0.0	7.9	0.0	0.0	0.0
CoreState	0.0	44.5	0.0	0.0	44.5	0.0	44.5	0.0	0.0	44.5	0.0	44.5	0.0	0.0
PreferentialAccess	4.0	31.8	4.0	7.9	35.8	11.9	39.7	4.0	7.9	35.8	11.9	39.7	4.0	0.0
LMRIntegration	15.9	127.1	15.9	31.8	143.0	47.7	158.9	15.9	31.8	143.0	47.7	158.9	15.9	31.8
OSSBSS	39.7	317.8	0.0	39.7	317.8	39.7	317.8	0.0	39.7	317.8	39.7	317.8	0.0	0.0
Handset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
RuggedisedHandset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
IVModem	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Spectrum	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	16.7	16.7	16.7	16.7	16.7	16.7	16.7	16.7	16.7	16.7	80.3	80.3
CoreNetworkAugmentation	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3
BackhaulUrban	1 048.1	1 048.1	631.1	901.5	901.5	901.5	901.5	688.3	983.3	983.3	983.3	983.3	456.8	137.0
BackhaulRegional	737.2	737.2	516.0	737.2	737.2	737.2	737.2	564.8	564.8	564.8	564.8	564.8	611.5	474.7
SiteLeasingUrban	1 244.6	1 244.6	1 070.6	1 070.6	1 070.6	1 070.6	1 070.6	1 167.6	1 167.6	1 167.6	1 167.6	1 167.6	0.0	0.0
SiteLeasingRegional	560.3	560.3	560.3	560.3	560.3	560.3	560.3	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Total operating costs	4 316.1	4 769.8	3 414.2	3 973.3	4 427.0	3 976.4	4 430.1	2 877.3	3 239.9	3 693.5	3 242.6	3 696.3	1 218.2	762.5

[a] National approach. [b] State-by-state approach.

Table C.44 **Net present value of costs (lower bound backhaul rental costs)**

$ millions

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Total costs														
Total	5 713.3	7 129.5	4 811.5	5 402.1	6 818.3	5 411.8	6 828.0	4 050.7	4 482.8	5 899.0	4 491.3	5 907.5	1 846.5	1 870.7
Capital Expenditure														
NewSiteBuildMetro	70.7	70.7	60.8	60.8	60.8	60.8	60.8	65.9	65.9	65.9	65.9	65.9	0.0	0.0
NewSiteBuildRegional	39.9	39.9	39.9	39.9	39.9	39.9	39.9	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	1 039.3	1 039.3	947.1	947.1	947.1	947.1	947.1	626.0	626.0	626.0	626.0	626.0	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	51.6	51.6	51.6	38.7	38.7	103.0	77.3
Battery24	155.9	155.9	142.1	142.1	142.1	106.6	106.6	93.9	93.9	93.9	70.4	70.4	0.0	0.0
Civil	18.4	18.4	16.8	16.8	16.8	16.8	16.8	18.2	18.2	18.2	18.2	18.2	14.3	14.3
CoreNational	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	0.0
CoreState	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0
PreferentialAccess	8.4	67.4	8.4	16.9	75.9	25.3	84.3	8.4	16.9	75.9	25.3	84.3	8.4	16.9
LMRIntegration	33.7	269.7	33.7	67.4	303.4	101.1	337.1	33.7	67.4	303.4	101.1	337.1	33.7	67.4
OSSBSS	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	0.0
Handset	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2
RuggedisedHandset	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5
IVModem	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1
Spectrum	263.6	263.6	263.6	263.6	263.6	263.6	263.6	224.0	224.0	224.0	224.0	224.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	170.6	170.6
CoreNetworkAugmentation	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8
Total capital expenditure	2 265.7	3 228.2	2 082.5	2 225.8	3 188.3	2 232.4	3 194.9	1 691.9	1 835.2	2 797.7	1 841.0	2 803.5	864.8	881.2

[a] National approach. [b] State-by-state approach.

(continued next page)

Table C.44 (continued)

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Operating costs														
NewSiteBuildMetro	59.0	59.0	50.7	50.7	50.7	50.7	50.7	55.3	55.3	55.3	55.3	55.3	0.0	0.0
NewSiteBuildRegional	33.2	33.2	33.2	33.2	33.2	33.2	33.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	491.3	491.3	447.4	447.4	447.4	447.4	447.4	295.0	295.0	295.0	295.0	295.0	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	24.2	24.2	24.2	18.2	18.2	48.4	36.3
Battery24	73.7	73.7	67.1	67.1	67.1	50.3	50.3	44.2	44.2	44.2	33.2	33.2	0.0	0.0
Civil	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
CoreNational	7.9	0.0	0.0	7.9	0.0	7.9	0.0	0.0	7.9	0.0	7.9	0.0	0.0	0.0
CoreState	0.0	44.5	0.0	0.0	44.5	0.0	44.5	0.0	0.0	44.5	0.0	44.5	0.0	0.0
PreferentialAccess	4.0	31.8	4.0	7.9	35.8	11.9	39.7	4.0	7.9	35.8	11.9	39.7	4.0	7.9
LMRIntegration	15.9	127.1	15.9	31.8	143.0	47.7	158.9	15.9	31.8	143.0	47.7	158.9	15.9	31.8
OSSBSS	39.7	317.8	0.0	39.7	317.8	39.7	317.8	0.0	39.7	317.8	39.7	317.8	0.0	0.0
Handset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
RuggedisedHandset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
IVModem	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Spectrum	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	16.7	16.7	16.7	16.7	16.7	16.7	16.7	16.7	16.7	16.7	80.3	80.3
CoreNetworkAugmentation	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3
BackhaulUrban	786.0	786.0	473.3	676.2	676.2	676.2	676.2	516.2	737.5	737.5	737.5	737.5	342.6	342.6
BackhaulRegional	589.7	589.7	412.8	589.7	589.7	589.7	589.7	451.8	451.8	451.8	451.8	451.8	489.2	489.2
SiteLeasingUrban	995.7	995.7	856.5	856.5	856.5	856.5	856.5	934.1	934.1	934.1	934.1	934.1	0.0	0.0
SiteLeasingRegional	350.2	350.2	350.2	350.2	350.2	350.2	350.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Total operating costs	3 447.6	3 901.3	2 729.0	3 176.3	3 630.0	3 179.4	3 633.1	2 358.8	2 647.5	3 101.2	2 650.3	3 104.0	981.7	989.5

[a] National approach. [b] State-by-state approach.

Table C.45 **Net present value of costs (upper bound backhaul rental costs)**
$ millions

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Total costs														
Total	6 532.2	7 948.4	5 333.5	6 147.7	7 563.9	6 157.5	7 573.7	4 620.8	5 200.3	6 616.5	5 208.8	6 625.0	2 319.5	2 343.7
Capital Expenditure														
NewSiteBuildMetro	70.7	70.7	60.8	60.8	60.8	60.8	60.8	65.9	65.9	65.9	65.9	65.9	0.0	0.0
NewSiteBuildRegional	39.9	39.9	39.9	39.9	39.9	39.9	39.9	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	1 039.3	1 039.3	947.1	947.1	947.1	947.1	947.1	626.0	626.0	626.0	626.0	626.0	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	51.6	51.6	51.6	38.7	38.7	103.0	77.3
Battery24	155.9	155.9	142.1	142.1	142.1	106.6	106.6	93.9	93.9	93.9	70.4	70.4	0.0	0.0
Civil	18.4	18.4	16.8	16.8	16.8	16.8	16.8	18.2	18.2	18.2	18.2	18.2	14.3	14.3
CoreNational	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	0.0
CoreState	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0
PreferentialAccess	8.4	67.4	8.4	16.9	75.9	25.3	84.3	8.4	16.9	75.9	25.3	84.3	8.4	16.9
LMRIntegration	33.7	269.7	33.7	67.4	303.4	101.1	337.1	33.7	67.4	303.4	101.1	337.1	33.7	67.4
OSSBSS	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	0.0
Handset	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2
RuggedisedHandset	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5
IVModem	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1
Spectrum	263.6	263.6	263.6	263.6	263.6	263.6	263.6	224.0	224.0	224.0	224.0	224.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	35.5	170.6	170.6
CoreNetworkAugmentation	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8
Total capital expenditure	2 265.7	3 228.2	2 082.5	2 225.8	3 188.3	2 232.4	3 194.9	1 691.9	1 835.2	2 797.7	1 841.0	2 803.5	864.8	881.2

[a] National approach. [b] State-by-state approach.

(continued next page)

Table C.45 (continued)

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Operating costs														
NewSiteBuildMetro	59.0	59.0	50.7	50.7	50.7	50.7	50.7	55.3	55.3	55.3	55.3	55.3	0.0	0.0
NewSiteBuildRegional	33.2	33.2	33.2	33.2	33.2	33.2	33.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	491.3	491.3	447.4	447.4	447.4	447.4	447.4	295.0	295.0	295.0	295.0	295.0	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	24.2	24.2	24.2	18.2	18.2	48.4	36.3
Battery24	73.7	73.7	67.1	67.1	67.1	50.3	50.3	44.2	44.2	44.2	33.2	33.2	0.0	0.0
Civil	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
CoreNational	7.9	0.0	0.0	7.9	0.0	7.9	0.0	0.0	7.9	0.0	7.9	0.0	0.0	0.0
CoreState	0.0	44.5	0.0	0.0	44.5	0.0	44.5	0.0	0.0	44.5	0.0	44.5	0.0	0.0
PreferentialAccess	4.0	31.8	4.0	7.9	35.8	11.9	39.7	4.0	7.9	35.8	11.9	39.7	4.0	7.9
LMRIntegration	15.9	127.1	15.9	31.8	143.0	47.7	158.9	15.9	31.8	143.0	47.7	158.9	15.9	31.8
OSSBSS	39.7	317.8	0.0	39.7	317.8	39.7	317.8	0.0	39.7	317.8	39.7	317.8	0.0	0.0
Handset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
RuggedisedHandset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
IVModem	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Spectrum	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	16.7	16.7	16.7	16.7	16.7	16.7	16.7	16.7	16.7	16.7	80.3	80.3
CoreNetworkAugmentation	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3
BackhaulUrban	1 310.1	1 310.1	788.9	1 126.9	1 126.9	1 126.9	1 126.9	860.4	1 229.1	1 229.1	1 229.1	1 229.1	571.0	571.0
BackhaulRegional	884.6	884.6	619.2	884.6	884.6	884.6	884.6	677.8	677.8	677.8	677.8	677.8	733.8	733.8
SiteLeasingUrban	995.7	995.7	856.5	856.5	856.5	856.5	856.5	934.1	934.1	934.1	934.1	934.1	0.0	0.0
SiteLeasingRegional	350.2	350.2	350.2	350.2	350.2	350.2	350.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Total operating costs	4 266.5	4 720.2	3 251.0	3 922.0	4 375.6	3 925.0	4 378.7	2 928.8	3 365.1	3 818.8	3 367.9	3 821.5	1 454.7	1 462.5

[a] National approach. [b] State-by-state approach.

Best and worst case scenario analysis

The best and worst case scenario analysis was conducted by varying multiple variables simultaneously, holding all other inputs constant. These variables are:

- the quantum of dedicated spectrum
- the opportunity cost of spectrum
- the number greenfield sites
- the cost of site equipment
- the cost of greenfield site builds
- network operating costs
- site leasing costs
- backhaul rental costs.

The results of the best and worst case scenario analysis are presented in tables C.46 and C.47 respectively.

Table C.46 **Net present value of costs (best case scenario)**
$ millions

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Total costs														
Total	4 390.1	5 655.1	3 590.9	4 159.0	5 424.0	4 171.7	5 432.7	3 161.1	3 570.6	4 835.6	3 578.2	4 843.2	1 712.5	1 734.0
Capital Expenditure														
NewSiteBuildMetro	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
NewSiteBuildRegional	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	649.6	649.6	591.9	591.9	591.9	591.9	591.9	391.3	391.3	391.3	391.3	391.3	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	51.6	51.6	51.6	38.7	38.7	103.0	77.3
Battery24	155.9	155.9	142.1	142.1	142.1	106.6	106.6	93.9	93.9	93.9	70.4	70.4	0.0	0.0
Civil	18.4	18.4	16.8	16.8	16.8	16.8	16.8	18.2	18.2	18.2	18.2	18.2	14.3	14.3
CoreNational	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	0.0
CoreState	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0
PreferentialAccess	8.4	67.4	8.4	16.9	75.9	25.3	84.3	8.4	16.9	75.9	25.3	84.3	8.4	16.9
LMRIntegration	33.7	269.7	33.7	67.4	303.4	101.1	337.1	33.7	67.4	303.4	101.1	337.1	33.7	67.4
OSSBSS	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	0.0
Handset	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2
RuggedisedHandset	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5
IVModem	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1
Spectrum	131.8	131.8	131.8	131.8	131.8	131.8	131.8	112.0	112.0	112.0	112.0	112.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	22.2	22.2	22.2	22.2	22.2	22.2	22.2	22.2	22.2	22.2	106.6	106.6
CoreNetworkAugmentation	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8
Total capital expenditure	1 633.6	2 596.1	1 481.6	1 624.8	2 587.4	1 631.5	2 594.0	1 266.0	1 409.2	2 371.8	1 415.0	2 377.5	800.8	817.2

[a] National approach. [b] State-by-state approach.

(continued next page)

Table C.46 **(continued)**

Option	*1*[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Operating costs														
NewSiteBuildMetro	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
NewSiteBuildRegional	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	204.7	204.7	186.4	186.4	186.4	186.4	186.4	122.9	122.9	122.9	122.9	122.9	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	16.1	16.1	16.1	12.1	12.1	32.3	24.2
Battery24	49.1	49.1	44.7	44.7	44.7	33.6	33.6	29.5	29.5	29.5	22.1	22.1	0.0	0.0
Civil	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
CoreNational	5.3	0.0	0.0	5.3	0.0	5.3	0.0	0.0	5.3	0.0	5.3	0.0	0.0	0.0
CoreState	0.0	29.7	0.0	0.0	29.7	0.0	29.7	0.0	0.0	29.7	0.0	29.7	0.0	0.0
PreferentialAccess	2.6	21.2	2.6	5.3	23.8	11.9	26.5	2.6	5.3	23.8	7.9	26.5	2.6	5.3
LMRIntegration	10.6	84.8	10.6	21.2	95.3	31.8	105.9	10.6	21.2	95.3	31.8	105.9	10.6	21.2
OSSBSS	26.5	211.9	0.0	26.5	211.9	26.5	211.9	0.0	26.5	211.9	26.5	211.9	0.0	0.0
Handset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
RuggedisedHandset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
IVModem	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Spectrum	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	7.0	7.0	7.0	7.0	7.0	7.0	7.0	7.0	7.0	7.0	33.5	33.5
CoreNetworkAugmentation	0.9	0.9	0.9	0.9	0.9	0.9	0.9	0.9	0.9	0.9	0.9	0.9	0.9	0.9
BackhaulUrban	786.0	786.0	473.3	676.2	676.2	676.2	676.2	516.2	737.5	737.5	737.5	737.5	342.6	342.6
BackhaulRegional	589.7	589.7	412.8	589.7	589.7	589.7	589.7	451.8	451.8	451.8	451.8	451.8	489.2	489.2
SiteLeasingUrban	786.0	786.0	676.2	676.2	676.2	676.2	676.2	737.5	737.5	737.5	737.5	737.5	0.0	0.0
SiteLeasingRegional	294.9	294.9	294.9	294.9	294.9	294.9	294.9	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Total operating costs	2 756.5	3 058.9	2 109.4	2 534.2	2 836.6	2 540.2	2 838.7	1 895.1	2 161.4	2 463.8	2 163.2	2 465.7	911.7	916.9

[a] National approach. [b] State-by-state approach.

Table C.47 **Net present value of costs (worst case scenario)**

$ millions

	1[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Total costs														
Total	8 797.0	10 364.4	7 432.3	8 269.1	9 836.5	8 279.8	9 847.2	5 987.1	6 589.2	8 156.6	6 598.6	8 166.0	2 508.3	2 535.1
Capital Expenditure														
NewSiteBuildMetro	318.1	318.1	273.7	273.7	273.7	273.7	273.7	296.6	296.6	296.6	296.6	296.6	0.0	0.0
NewSiteBuildRegional	179.5	179.5	179.5	179.5	179.5	179.5	179.5	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	1 558.9	1 558.9	1 420.7	1 420.7	1 420.7	1 420.7	1 420.7	939.0	939.0	939.0	939.0	939.0	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	51.6	51.6	51.6	38.7	38.7	103.0	77.3
Battery24	155.9	155.9	142.1	142.1	142.1	106.6	106.6	93.9	93.9	93.9	70.4	70.4	0.0	0.0
Civil	18.4	18.4	16.8	16.8	16.8	16.8	16.8	18.2	18.2	18.2	18.2	18.2	14.3	14.3
CoreNational	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	16.9	0.0	16.9	0.0	0.0	0.0
CoreState	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0	94.4	0.0	94.4	0.0	0.0
PreferentialAccess	8.4	67.4	8.4	16.9	75.9	25.3	84.3	8.4	16.9	75.9	25.3	84.3	8.4	16.9
LMRIntegration	33.7	269.7	33.7	67.4	303.4	101.1	337.1	33.7	67.4	303.4	101.1	337.1	33.7	67.4
OSSBSS	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	84.3	674.3	84.3	674.3	0.0	0.0
Handset	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2	126.2
RuggedisedHandset	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5	253.5
IVModem	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1	152.1
Spectrum	353.2	353.2	353.2	353.2	353.2	353.2	353.2	300.2	300.2	300.2	300.2	300.2	0.0	0.0
MNOSitesAugmentation	0.0	0.0	53.2	53.2	53.2	53.2	53.2	53.2	53.2	53.2	53.2	53.2	255.9	255.9
CoreNetworkAugmentation	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8
Total capital expenditure	3 261.9	4 224.5	3 015.8	3 159.1	4 121.6	3 165.7	4 128.3	2 329.6	2 472.8	3 435.4	2 478.6	3 441.1	950.1	966.5

[a] National approach. [b] State-by-state approach.

(continued next page)

Table C.47 **(continued)**

	1[a]	*1*[b]	*2a*[a]	*2b*[a]	*2b*[b]	*2c*[a]	*2c*[b]	*3a*[a]	*3b*[a]	*3b*[b]	*3c*[a]	*3c*[b]	*4a*[a]	*4b*[a]
Operating costs														
NewSiteBuildMetro	353.7	353.7	304.3	304.3	304.3	304.3	304.3	331.9	331.9	331.9	331.9	331.9	0.0	0.0
NewSiteBuildRegional	199.0	199.0	199.0	199.0	199.0	199.0	199.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
SiteEquipment	982.7	982.7	894.8	894.8	894.8	894.8	894.8	590.0	590.0	590.0	590.0	590.0	0.0	0.0
Battery20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	32.3	32.3	32.3	24.2	24.2	64.6	48.4
Battery24	98.3	98.3	89.5	89.5	89.5	67.1	67.1	59.0	59.0	59.0	44.2	44.2	0.0	0.0
Civil	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
CoreNational	10.6	0.0	0.0	10.6	0.0	10.6	0.0	0.0	10.6	0.0	10.6	0.0	0.0	0.0
CoreState	0.0	59.3	0.0	0.0	59.3	0.0	59.3	0.0	0.0	59.3	0.0	59.3	0.0	0.0
PreferentialAccess	5.3	42.4	5.3	10.6	47.7	15.9	53.0	5.3	10.6	47.7	15.9	53.0	5.3	10.6
LMRIntegration	21.2	169.5	21.2	42.4	190.7	63.6	211.9	21.2	42.4	190.7	63.6	211.9	21.2	42.4
OSSBSS	53.0	423.8	0.0	53.0	423.8	53.0	423.8	0.0	53.0	423.8	53.0	423.8	0.0	0.0
Handset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
RuggedisedHandset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
IVModem	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Spectrum	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
MNOSitesAugmentation	0.0	0.0	33.4	33.4	33.4	33.4	33.4	33.4	33.4	33.4	33.4	33.4	160.6	160.6
CoreNetworkAugmentation	1.7	1.7	1.7	1.7	1.7	1.7	1.7	1.7	1.7	1.7	1.7	1.7	1.7	1.7
BackhaulUrban	1 310.1	1 310.1	788.9	1 126.9	1 126.9	1 126.9	1 126.9	860.4	1 229.1	1 229.1	1 229.1	1 229.1	571.0	571.0
BackhaulRegional	884.6	884.6	619.2	884.6	884.6	884.6	884.6	677.8	677.8	677.8	677.8	677.8	733.8	733.8
SiteLeasingUrban	1 113.6	1 113.6	957.9	957.9	957.9	957.9	957.9	1 044.7	1 044.7	1 044.7	1 044.7	1 044.7	0.0	0.0
SiteLeasingRegional	501.3	501.3	501.3	501.3	501.3	501.3	501.3	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Total operating costs	5 535.0	6 139.9	4 416.4	5 109.9	5 714.9	5 114.1	5 719.0	3 657.6	4 116.3	4 721.3	4 120.0	4 724.9	1 558.2	1 568.6

[a] National approach. [b] State-by-state approach.

C.9 Excluded costs

Certain costs are excluded from the quantitative analysis. Generally, this is because there is insufficient information by which to assess the magnitude of these costs or whether the costs would be realised and because these costs are unlikely to vary significantly between options. It is likely that many of these costs will be substantial but, given the limitations of this study, they are impossible to assess or would be unlikely to alter the ranking of options.

It is expected that some of these cost items will be revisited for the final report. The Commission is seeking feedback on whether and how these items should be included.

Alternative or supplementary technologies

The cost of alternative or supplementary communication services, such as deployables, satellite technology and other non-permanent networks, have not been included in the analysis. In general, these solutions are used to provide coverage or additional capacity in exceptional circumstances where the permanent RAN network is absent or insufficient. Consequently, the demand for these technologies depends crucially on the frequency, magnitude and location of peaks in traffic demand, for which empirical evidence and robust forecasts are virtually nonexistent.

Moreover, given that, by construction, the permanent network under all options delivers the same baseline level of capacity and coverage, it is unlikely that the cost of alternative or supplementary networks would vary significantly between options from the community's perspective (the costs to specific parties, such as mobile carriers and PSAs, could differ).

Value of spectrum sharing

As discussed above, some options include a dedicated network, which must be supported by dedicated spectrum. In these cases, the opportunity cost for that spectrum comprises part of the total cost of the network.

However, under some options (namely, the hybrid and dedicated options) there is scope for this cost to be mitigated if that spectrum is shared with other users. For example, in periods of low PSA traffic, the spectrum could be used to carry commercial traffic.

In the absence of reliable traffic forecasts for PSAs and detailed information relating to other traffic, it is impossible to predict how much excess capacity there would be in the dedicated spectrum bands, and to what extent that capacity could usefully be shared with other mobile broadband users.

Cost of developing applications

Under all options, the use of the PSMB network will require the development of new applications that meet PSA requirements, including standards relating to security and interoperability. These costs are likely to be similar under all options and therefore have not been accounted for in the quantitative analysis.

Common organisational-level costs

Common organisational-level costs have been omitted from the calculation of costs. These refer to costs that are common to all areas of a mobile carrier's business, such as management salaries, head-office administration, the cost of operating data centres and backend IT systems.

For mobile carrier networks, these costs are likely to be invariant to additional traffic (Ofcom 2006). As a result, the incremental cost of adding PSAs to the network will likely be close to zero. By contrast, some of these costs will form part of the incremental costs of a dedicated network. For example, the cost of establishing a head office will be incurred anew.

However, on a practical level, estimating these costs is difficult due to the lack of publically available data relating to the materiality of these costs. Nevertheless, it is assumed that the magnitude of these costs would be unlikely to change the relative rankings of different delivery options.

Costs of trunk backhaul transmission (including inter-capital transmission)

As noted in section C.5, a simplified approach has been taken to estimating backhaul costs via a representative per-site cost that captures backhaul capacity from each mobile site back to some point of aggregation, based on assumptions about the average distance and level of capacity required. These estimates also factor in an annualised cost for new backhaul links for a proportion of sites to increase the level of geographic diversity.

Some costs associated with backhaul capacity (such as trunk backhaul between major regional centres, and inter-capital transmission) may not be captured by these cost estimates. Given the level of uncertainty associated with how a carrier would structure the topology of its network to deliver a PSMB capability, the analysis has not sought to include these costs explicitly.

Cost of change

The costs of transitioning from current PSA networks to PSMB has been excluded from the analysis. These costs include the cost of instituting regulatory and governance arrangements, the transaction costs associated with tendering and procurement, and the opportunity cost of developing or changing PSA protocols and practices, including training and other change management.

For the most part, these costs are intangible and hence inherently difficult to quantify. Moreover, these costs are likely to be, in broad terms, common across the delivery options and there is scant evidence as to how these might differ quantitatively between the options.

Externality effects

Except to the extent discussed in this section, the external costs and benefits of providing a PSMB capability via different options have been excluded. These include any deterioration in service quality or congestion experienced by commercial mobile broadband customers as a result of adding PSA users to commercial networks. They also include any spillover benefits these customers might experience as a result of upgrades made to commercial networks.

References

3GPP (3rd Generation Partnership Project) 2013, *Delivering Public Safety Communications with LTE*, www.3gpp.org/news-events/3gpp-news/1455-Public-Safety (accessed 26 August 2015).

—— 2015a, *3GPP Feature and Study Item list: Rel-14*, www.3gpp.org/DynaReport/FeatureListFrameSet.htm (accessed 26 August 2015).

—— 2015b, *3GPP, The Mobile Broadband Standard*, www.3gpp.org (accessed 26 August 2015).

—— 2015c, *About 3GPP Home*, www.3gpp.org/about-3gpp/about-3gpp (accessed 26 August 2015).

—— 2015d, *SA6: Mission-Critical Applications*, www.3gpp.org/specifications-groups/sa-plenary/sa6-mission-critical-applications (accessed 26 August 2015).

—— 2015e, *Tentative 3GPP Timeline for 5G*, www.3gpp.org/news-events/3gpp-news/1674-timeline_5g (accessed 26 August 2015).

4G Americas 2013, *Self-Optimising Networks in 3GPP Release 11: The Benefits of SON in LTE*, White Paper, Bellevue, Washington, United States.

ABS (Australian Bureau of Statistics) 2014, *Australian Population Grid 2011*, Cat no. 1270.0.55.007, Canberra.

ACCAN (Australian Communications Consumer Action Network) 2014, *Warrnambool Exchange Fire Consumer Impact Analysis*, https://accan.org.au/grants/completed-grants/623-warrnambool-exchange-fire-consumer-impact-analysis (accessed 26 August 2015).

ACCC (Australian Competition and Consumer Commission) 2013, *Facilities Access Code Final Decision*, Canberra.

—— 2014a, *Domestic Transmission Capacity Service*, Final Report, Canberra.

—— 2014b, *Mobile Terminating Access Service*, Final Access Determination Discussion Paper, Canberra.

—— 2015a, *Public Inquiry to make a Final Access Determination for the Domestic Transmission Capacity Service*, Draft Decision, Canberra.

—— 2015b, *Telecommunications Competitive Safeguards for 2013-14*, Report to the Minister for Communications, Canberra.

Access Economics 2010, *Radiofrequency Spectrum Options for Public Safety Agencies*, Attorney-General's Department, Canberra.

Acer Computer 2014, *Tasmania Police mobile in the community with Acer windows 8 tablets*, Media Release, 4 December.

ACMA (Australian Communications and Media Authority) 2009, *Australian Radiofrequency Spectrum Allocations Chart*, www.acma.gov.au/webwr/radcomm/frequency_planning/spectrum_plan/aust_rf_spectrum_allocations_chart.pdf (accessed 24 June 2015).

—— 2012a, *Spectrum for Public Safety Radiocommunications: Current ACMA Initiatives and Decisions*, Canberra.

—— 2012b, *The 803–960 MHz Band: Exploring Options for Future Change*, Discussion Paper, Canberra.

—— 2013a, *Apparatus Licence Periods*, www.acma.gov.au/Industry/Spectrum/Radiocomms-licensing/Apparatus-licences/apparatus-licence-periods-apparatus-licensing-acma (accessed 26 August 2015).

—— 2013b, *Australian Spectrum Management Principles*, www.acma.gov.au/Industry/Spectrum/Spectrum-planning/About-spectrum-planning/australian-spectrum-management-principles-spectrum-planning-acma (accessed 24 June 2015).

—— 2013c, *Spectrum Licensing FAQs*, www.acma.gov.au/Industry/Spectrum/Radiocomms-licensing/Spectrum-licences/spectrum_20 (accessed 26 August 2015).

—— 2013d, *Supplementary Submission to 'Spectrum for Public Safety Mobile Broadband'*, Canberra.

—— 2014a, *400 MHz Implementation FAQs*, www.acma.gov.au/Industry/Spectrum/Spectrum-projects/400-MHz-band/400-mhz-implementation-faqs (accessed 9 September 2015).

—— 2014b, *ACMA Mobile Network Capacity Forecasting Model: User Guide*, Canberra.

—— 2014c, *Communications Report 2013-14*, Canberra.

—— 2014d, *Introduction to the ACMA*, www.acma.gov.au/theACMA/About/The-ACMA-story/Communicating/introduction-to-the-acma (accessed 9 September 2015).

—— 2014e, *Land Mobile Licences: Guidelines*, www.acma.gov.au/theACMA/land-mobile-licences-guidelines (accessed 24 June 2015).

—— 2014f, *Third-Party Authorisation*, www.acma.gov.au/Industry/Spectrum/Radiocomms-licensing/Apparatus-licences/third-party-authorisation-apparatus-licences-acma (accessed 27 August 2015).

—— 2014g, *Wireless LANs in the 2.4 GHz Band FAQ*, http://acma.gov.au/Citizen/Consumer-info/My-connected-home/Wireless-local-area-networks/wireless-lans-in-the-24-ghz-band-faqs (accessed 24 June 2015).

—— 2015a, *Apparatus Licensing System*, www.acma.gov.au/Industry/Spectrum/Radiocomms-licensing/Apparatus-licences/apparatus-licensing-system-acquire-a-licence-acma (accessed 27 August 2015).

—— 2015b, *Milestone Transition Timeline*, www.acma.gov.au/Industry/Spectrum/Spectrum-projects/400-MHz-band/milestone-transition-timeline (accessed 24 June 2015).

—— 2015c, *Monitoring Milestone Two*, www.acma.gov.au/Industry/Spectrum/Spectrum-projects/400-MHz-band/monitoring-milestone-two (accessed 24 June 2015).

—— 2015d, *Progressing Opportunity Cost Pricing in the 400 MHz Band*, www.acma.gov.au/Industry/Spectrum/Spectrum-projects/400-MHz-band/progressing-opportunity-cost-pricing-in-the-400-mhz-band (accessed 28 August 2015).

—— 2015e, *Radiocomms Licence Data on CD-ROM*, www.acma.gov.au/Industry/Spectrum/Radiocomms-licensing/Register-of-radiocommunications-licences/radiocomms-licence-data (accessed 27 August 2015).

ACT Government, NSW Government, Queensland Government, Government of South Australia, Tasmanian Government, Victorian Government and Government of Western Australia 2013, *Public Safety Mobile Broadband Joint States and Territories Submission to the Standing Council on Police and Emergency Management and the Australian Communications and Media Authority: Further Evidence from Jurisdictions*, Canberra.

Adobe nd, *Table 1. Recommended Bit Rates for Live Streaming*, www.adobe.com/devnet/adobe-media-server/articles/dynstream_live/popup.html (accessed 2 September 2015).

Airbus Group 2015, *New Solution Complements Existing Tetra Public safety radio network VIRVE by using commercial broadband mobile networks*, www.airbusgroup.com/int/en/news-media/press-releases/Airbus-Group/Financial_Communication/2015/02/20150226_airbus_defence_and_space_tactilon.html (accessed 26 August 2015).

Alcatel-Lucent 2009, *The LTE Network Architecture: A Comprehensive Tutorial*, Strategic White Paper, Sydney.

—— 2010, *Network Sharing in LTE: Opportunity and Solutions*, Slide Share, www.slideshare.net/allabout4g/lte-network-sharing (accessed 31 August 2015).

Analysys Mason 2010, *Public Safety Mobile Broadband and Spectrum Needs*, Final Report for the TETRA Association, London.

—— 2012, *Impact of Radio Spectrum on the UK Economy and Factors Influencing Future Spectrum Demand*, Report for the Department for Business, Innovation and Skills and Department for Culture, Media and Sport, London.

—— 2015, *Mobile Network Infrastructure Forecasts*, Updated Final Report for the Australian Communications and Media Authority, London.

APCO (Association of Public-Safety Communications Officials Australasia) 2011, *APCO Global Alliance Adopts LTE as International Public Safety Standard*, Media release, 20 April, Melbourne.

ASTRID 2011a, *Blue Light Mobile: 1 Operator, 3 Networks*, www.astrid.be/templates/content.aspx?id=7058&LangType=1033 (accessed 26 August 2015).

—— 2011b, *Digital Radio Communications*, www.astrid.be/templates/content.aspx?id=3714&LangType=1033 (accessed 26 August 2015).

—— 2011c, *Legal Framework*, www.astrid.be/templates/content.aspx?id=3842 (accessed 26 August 2015).

—— 2014a, *Access and Security*, http://bluelightmobile.be/en/access-and-security (accessed 26 August 2015).

—— 2014b, *Bluelight Mobile FAQ*, http://bluelightmobile.be/en/faq (accessed 26 August 2015).

Attorney-General's Department 2011, *Public Safety Mobile Broadband Steering Committee Terms of Reference*, Canberra.

Australian Emergency Management Institute 2011, *National Strategy for Disaster Resilience*, https://www.em.gov.au/Publications/Program%20publications/Pages/NationalStrategyforDisasterResilience.aspx (accessed 24 June 2015).

Baker, R. and Ruting, B. 2014, *Environmental Policy Analysis: A Guide to Non-Market Valuation*, Productivity Commission Staff Working Paper, Productivity Commission, Canberra.

Bell Labs 2011, *High Level Total Cost of Ownership Comparison: Stand Alone Public Safety Network vs. Public Private Partnership*, Alcatel-Lucent, Murray Hill, New Jersey, United States.

Borkar, S., Robertson, D. and Zdunek, K. 2011, *Public Safety Priority Access to Shared Commercial Networks*, Roberson and Associates, Schaumburg, Illinois, United States.

Brinkmann, M., Hackbarth, K., Ilic, D., Neu, W., Neumann, K.-H. and Figueras, A.P. 2007, *Mobile Termination Cost Model for Australia*, Report for the Australian Competition and Consumer Commission, WIK Consult, Bad Honnef, Germany.

Brydon, A. 2012, *Summary of 3GPP Standards Releases for LTE*, *Wireless Blog from Unwired Insight*, 5 October, www.unwiredinsight.com/2012/3GPP-LTE-releases (accessed 9 September 2015).

Carney, B., King, S. and Maddock, R. 2015, *Reforming Free-to-Air Broadcasting in Australia*, Monash Business School, Melbourne.

Chan, C., Forwood, D., Roper, H. and Sayers, C. 2009a, *Public Infrastructure Financing: An International Perspective*, Productivity Commission Staff Working Paper, Productivity Commission, Canberra.

Chan, C., Roper, H., Forwood, D. and Sayers, C. 2009b, *Public Infrastructure Financing - An International Perspective*, Staff Working Paper, Productivity Commission.

CIE (Centre for International Economics) 2014, *The Economic Impacts of Mobile Broadband on the Australian Economy, from 2006 to 2013*, Research Report prepared for the Australian Communications and Media Authority, Canberra.

Clemons, P. 2015, *The End of Airwave and the Truth About TETRA and LTE for UK Emergency Services (Act 2)*, TETRA Applications, www.tetra-applications.com/30060/weblog/the-end-of-airwave-and-the-truth-about-tetra-and-lte-for-uk-emergency-services-act-2 (accessed 27 August 2015).

COAG (Council of Australian Governments) 2009, *National Framework to Improve Government Radiocommunications Interoperability 2010–2020*, Canberra.

—— 2013, *Council of Australian Governments Meeting Communiqué Canberra, 19 April 2013*, Canberra.

—— 2015, *National Security and Community Safety*, https://www.coag.gov.au/national_security_and_community_safety (accessed 24 June 2015).

Cole, J. and Hawker, E. 2014, *Emergency Services Communications: Resilience for the Twenty-First Century*, British APCO and Royal United Services Institute, London.

Coleago Consulting 2015, *Mobile Network Infrastructure Sharing: Industry Overview and Coleago's Approach*, www.slideshare.net/fullscreen/StefanZehle/coleago-network-sharing-overview-v011-100215-cb/2 (accessed 7 September 2015).

Communications Alliance 2013, *Industry Guideline G596:2013 Communication Support for Emergency Response*, Sydney.

Competition Policy Review 2015, *Competition Policy Review Final Report*, Australian Government, Canberra.

Cornick, K. and Gathercole, B. 2012, *Broadband Communications Options for Public Safety Agencies*, Australian Broadband Applications Laboratory, Melbourne.

Cowan, P. 2014, 'Northern Territory to give every frontline cop an iPad', *IT News*, 5 February, www.itnews.com.au/News/371352,northern-territory-to-give-every-frontline-cop-an-ipad.aspx (accessed 28 August 2015).

Coyne, A. 2015, 'NSW police buys 500 Samsung Galaxy smartphones', *IT News*, 23 February, www.itnews.com.au/News/400805,nsw-police-buys-500-samsung-galaxy-smartphones.aspx (accessed 28 August 2015).

Critical Comms 2015, 'Motorola wins $175m deal to upgrade and manage SA's GRN', www.radiocomms.com.au/content/radios/news/motorola-wins-175m-deal-to-upgrade-and-manage-sa-39-s-grn-382236627 (accessed 8 September 2015).

CSS (Centre for Security Science) 2011, *700MHz Spectrum Requirements for Canadian Public Safety Interoperable Mobile Broadband Data Communications*, Defence Research and Development Canada, Ottawa.

—— 2013, *Public Safety Broadband Network Architecture Description*, Defence Research and Development Canada, Ottawa.

Delgado, M. 2010, 'Police told to send text messages because it is too expensive to speak on their radios', *Daily Mail Australia*, 14 November, www.dailymail.co.uk/news/article-1329538/Police-told-send-text-messages-expensive-speak-radios.html (accessed 8 September 2015).

Deloitte 2013, *Emergency Services Long Term Strategic Plan: International Public Safety Broadband*, Victorian Department of Justice, Melbourne.

Department of Communications 2014a, *Mobile Black Spot Programme Guidelines*, Version 1.1, Canberra.

—— 2014b, *Review of the National Triple Zero (000) Operator*, Discussion Paper, Canberra.

—— 2015a, *NBN Satellite Launch Date Announced*, https://www.communications.gov.au/departmental-news/nbn-satellite-launch-date-announced (accessed 9 September 2015).

—— 2015b, *Spectrum Review*, Canberra.

Department of Finance 2015, *Procurement of Air Travel Services for the Australian Government*, Discussion Paper, Canberra.

Department of Finance and Administration 2006, *Handbook of Cost-Benefit Analysis*, Financial Management Reference Material no. 6, Canberra.

ECC (Electronic Communications Committee) 2013, *User requirements and spectrum needs for future European broadband PPDR systems (Wide Area Networks)*, Report no. 199, Copenhagen.

ECRC (Environment and Communications References Committee) 2011, *The Capacity of Communication Networks and Emergency Warning Systems to Deal with Emergencies and Natural Disasters*, The Senate, Canberra.

Emergency Alert nd, *Emergency Alert: How Will it Work on Mobile Phones?*, www.emergencyalert.gov.au/frequently-asked-questions/how-will-it-work-on-mobile-phones.html (accessed 28 August 2015).

EMV (Emergency Management Victoria) 2014, *Victoria's Emergency Management Long Term Communications Plan*, Melbourne.

ENISA (European Network and Information Security Agency) 2011, *Measurement Frameworks and Metrics for Resilient Networks and Services: Technical Report*, Discussion Draft.

Ericsson 2013a, *Ericsson Mobility Report, June 2013*, Stockholm.

—— 2013b, *What is Backhaul? How will Backhaul Evolve?*, www.ericsson.com/res/thecompany/docs/press/backgrounders/press-backgrounder-backhaul.pdf (accessed 15 September 2015).

—— 2014a, *Microwave Towards 2020: Delivering High-Capacity and Cost-Efficient Backhaul for Broadband Networks Today and in the Future*, Stockholm.

—— 2014b, *Public Safety Mobile Broadband*, White Paper, Stockholm.

Ernst & Young 2011, *Benefit Cost Analysis of National Mobile Broadband Capacity for Emergency Services Organisations*, Victorian Department of Treasury and Finance, Melbourne.

Essid, C. 2012, *Nationwide Public Safety Broadband Network*, Office of Emergency Communications, US Department of Homeland Security, Washington DC.

ESTA (Emergency Services Telecommunications Authority) 2014a, *Annual Report 2013-14*, Victorian Government, Melbourne.

—— (Emergency Services Telecommunications Authority) 2014b, *The Mobile Data Network*, www.esta.vic.gov.au/None/MDN (accessed 28 August 2015).

FCC (Federal Communications Commission) 2010a, *A Broadband Network Cost Model*, OBI Technical Paper, Washington DC.

—— 2010b, *The Public Safety Nationwide Interoperable Broadband Network: A New Model for Capacity, Performance and Cost*, Washington DC.

—— 2012, *Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Public Safety Broadband Network*, Technical Advisory Board for First Responder Interoperability, Washington DC.

FirstNet 2015a, *About FirstNet*, www.firstnet.gov/about (accessed 26 August 2015).

—— 2015b, *Draft RFP*, Tallahassee, Florida, United States.

—— 2015c, *SOO Appendix C-1 Baseline Coverage Objective Maps*, www.floridanet.gov/assets/docs/FirstNet/2015_04_Draft_RFP/03%20-%20d15ps00295_c-1_coverage_maps.pdf (accessed 15 September 2015).

—— 2015d, *Statement of Objectives RFP*, Tallahassee, Florida, United States.

Ford, G. and Spiwak, L. 2011, 'Public safety or commercial use? A cost/benefit framework for the D block', Phoenix Center Policy Bulletin No. 26, Phoenix Center for Advanced Legal & Economic Public Policy Studies, Washington DC, pp. 1–15.

Fournier, J. 2015, '700 MHz Public Safety Broadband: Canada Update', presented at PSCR 2015 Public Safety Broadband Stakeholder Meeting, San Diego, June.

Francis, H. 2015, 'NSW Police goes high-tech ... with mobile phones', *The Age*, 23 February, www.theage.com.au/it-pro/government-it/nsw-police-goes-hightech--with-mobile-phones-20150223-13m2g4.html (accessed 24 June 2015).

Government of Canada 2015, *Strong Leadership: A Balanced-Budget, Low-Tax Plan for Jobs, Growth and Security*, Ottawa.

GQ-AAS (Gibson Quai AAS Consulting) 2010, *Public Safety High Speed Radiocommunications Options Analysis*, Attorney-General's Department, Canberra.

—— 2011a, *Interoperability Gateway Solutions*, Canberra.

—— 2011b, *Public Safety Mobile Broadband Demand Requirements: For Public Safety Mobile Broadband Steering Committee*, Attorney-General's Department, Canberra.

—— 2011c, *Public Safety Mobile Broadband Spectrum Quantum Calculation*, Attorney-General's Department, Canberra.

Gras, L. 2015, 'LTE roaming: issues, challenges, opportunities', *Techzine*, 3 January, https://techzine.alcatel-lucent.com/lte-roaming-issues-challenges-opportunities (accessed 8 September 2015).

Gregory, M., Scholfield, Kaye, Ahmed, K.E.U., McLaren, D. and Williams, J. 2014, 'Warrnambool exchange fire: Resilience and emergency management', *Australian Journal of Telecommunications and the Digital Economy*, vol. 2, no. 4.

Grous, A. 2013a, *Socioeconomic Value of Mission Critical Mobile Applications for Public Safety in the EU: 2x10MHz in 700MHz in 10 European Countries*, London School of Economics and Political Science, London.

—— 2013b, *Socioeconomic Value of Mission Critical Mobile Applications for Public Safety in the UK: 2x10MHz in 700MHz*, London School of Economics and Political Science, London.

GSC (Global Standards Collaboration) 2014, *Draft Report of the Global Standards Collaboration (GSC) Task Force on Emergency Communications*, Task Force Report, Geneva.

GSMA (GSM Association) 2012, *Mobile Infrastructure Sharing*, London.

Hallahan, R. and Peha, J.M. 2013, 'Enabling public safety priority use of commercial wireless networks', *Homeland Security Affairs*, vol. 9, no. 31, pp. 1–26.

IC (Industry Commission) 1996, *Competitive Tendering and Contracting By Public Sector Agencies*, Report no. 48, Canberra.

iiNet 2015, *Broadband2+ Speeds Explained*, www.iinet.net.au/iinetwork/bb2-speeds.html (accessed 8 September 2015).

Industry Canada 2012, *Consultation on a Policy, Technical and Licensing Framework for Use of the Public Safety Broadband Spectrum in the Bands 758-763 MHz and 788-793 MHz (D Block) and 763-768 MHz and 793-798 MHz (PSBB Block)*, Ottawa.

ITU (International Telecommunications Union) 2014, *The Use of International Mobile Telecommunications for Broadband Public Protection and Disaster Relief Applications*, Report no. M.2291, Geneva.

—— 2015, *ICT Facts & Figures: The world in 2015*, Geneva.

Jackson, D. 2014, *FirstNet looks to issue final RFP by the end of 2015*, Urgent Communications, http://urgentcomm.com/public-safety-broadbandfirstnet/firstnet-looks-issue-final-rfp-end-2015 (accessed 3 September 2015).

Key, J. (Prime Minister of New Zealand) 2013, *Police Roll Out New Technology to Fight Crime*, Media Release, 13 February, Wellington, https://www.national.org.nz/news/news/media-releases/detail/2013/02/12/police-roll-out-new-technology-to-fight-crime (accessed 28 August 2015).

Kidman, A. 2015, 'Telstra and Optus outline their speedy futures', *PC Mag*, http://au.pcmag.com/telstra/28777/news/telstra-and-optus-outline-their-speedy-futures (accessed 28 August 2015).

Kim, D. 2015, ‘Korea SafeNet and “LTE for Public Safety” Standardization’, presented at PSCR 2015 Public Safety Broadband Stakeholder Meeting, San Diego, 3 June.

LTE-Applications 2014, *South Korea Selects 700 MHz Band 28 for Public-Safety LTE Network*, www.lte-applications.com/27249/news/south-korea-selects-700-mhz-band-28-for-public-safety-lte-network (accessed 28 August 2015).

Mahindra, R., Khojastepour, M.A., Zhang, H. and Rangarajan, S. 2013, *Network-Wide Radio Access Network Sharing in Cellular Networks*, NEC Labratories, Princeton.

Metropolitan Ambulance Service 2004, ‘Perspective’, December 2004, www.ambulance.vic.gov.au/Media/docs/Perspective-November-2004-bb763319-14c2-4a30-a0df-f1919b25dee8-0.pdf (accessed 24 June 2015).

MFB (Metropolitan Fire Brigade) 2013, *Aerial Fire Fighting Tool Takes Off*, www.mfb.vic.gov.au/News/Aerial-fire-fighting-tool-takes-off.html (accessed 28 August 2015).

Minehane, S.W., Molloy, S. and Burgan, B. 2014, *Valuing Mission Critical Radio Services: Study of the Economic Value of Land Mobile Radio Spectrum in Australia*, Windor Place Consulting, Melbourne.

Mnookin, R.H. 2003, ‘Strategic barriers to dispute resolution: a comparison of bilateral and multilateral negotiations’, *Journal of Institutional and Theoretical Economics*, vol. 159, no. 1, pp. 199–220.

Moore, L.K. 2015, *The First Responder Network (FirstNet) and Next-Generation Communications for Public Safety: Issues for Congress*, CRS Report no. R42543, Congressional Research Service, Washington DC.

Moran, A. 2013, ‘New equipment for Ambulance Service’, Port Augusta, *The Transcontinental*, 8 May, www.transcontinental.com.au/story/1486797/new-equipment-for-ambulance-service/ (accessed 8 September 2015).

Motorola Solutions 2011, *Product Spec Sheet: HPD 1000 Data Modem for ASTRO 25 HPD Systems*, Schaumburg, Illinois, United States.

Nadiv, R. and Naveh, T. 2010, *Wireless Backhaul Topologies: Analyzing Backhaul Topology Strategies*, White Paper, Ceragon Networks Ltd., Tel Aviv.

Nally, J. 2014, *Rural radio: Victorian firefighters join the digital age*, Critical Comms, www.radiocomms.com.au/content/public-safety/article/rural-radio-victorian-firefighters-join-the-digital-age-40273033 (accessed 7 September 2015).

NBN Co 2014, *Fact Sheet: Satellite Support Scheme*, www.nbnco.com.au/content/dam/nbnco2/documents/satellite-support-scheme-fact-sheet.pdf (accessed 8 September 2015).

—— 2015a, *Integrated Product Roadmap as at April 2015*, Sydney.

—— 2015b, *NBN Satellite Support Scheme*, www.nbnco.com.au/connect-home-or-business/information-for-home-or-business/satellite.html (accessed 7 September 2015).

NEC 2013, *RAN Sharing: NECs Approach towards Active Radio Access Network Sharing*, White Paper, Tokyo.

NERA and Smith System Engineering 1996, *Study into the Use of Spectrum Pricing*, Radiocommunications Agency, London.

New Zealand Police 2014, *Policing Excellence: The Transformation of New Zealand Police 2009–2014*, Wellington.

NMC Consulting 2013, *LTE Handover*, www.nmcgroups.com/en/expertise/lte/x2handover.asp (accessed 1 September 2015).

Nokia Siemens Network 2010, *Mobile broadband with HSPA and LTE - capacity and cost aspects*, White Paper, Finland.

NPSTC (National Public Safety Telecommunications Council) 2012, *Priority and QoS in the Nationwide Public Safety Broadband Network*, Revision no. 1.0, Littleton, Colorado, United States.

—— 2014, *Defining Public Safety Grade Systems and Facilities*, Littleton, Colorado, United States.

—— and CITIG (Canadian Interoperability Technology Interest Group) 2015, *Cross Border Communications Report*, Canadian Interoperability Technology Interest Group, Kanata, Ontario.

NSW Legislative Council 2012, *Rail Infrastructure Project Costing in New South Wales*, Inquiry of the General Purpose Standing Committee no. 3, Sydney.

NSW Telco Authority 2014, *Annual Report 2013-14*, NSW Government, Sydney.

—— 2015, *Government Radio Network*, http://telco.nsw.gov.au/content/government-radio-network-grn (accessed 28 August 2015).

O'Farrell, B., Baillieu, T., Newman, C. and Barnett, C. 2012, *Letter to Prime Minister Julia Gillard MP*, www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/Completed_inquiries/2010-13/spectrummobilebroadband/submissions (accessed 28 August 2015).

OBPR (Office of Best Practice Regulation) 2014a, *Best Practice Regulation Guidance Note: Value of Statistical Life*, Department of the Prime Minister and Cabinet, Canberra.

—— 2014b, *Cost-Benefit Analysis Guidance Note*, Department of the Prime Minister and Cabinet, Canberra.

OECD (Organisation for Economic Co-operation and Development) 2014, *New Approaches to Spectrum Management*, OECD Digital Economy Papers no. 235, OECD Publishing, Paris.

Ofcom (Office of Communications) 2006, *Mobile Call Termination: Proposals for Consultation*, London.

OpenSignal 2015, *The State of LTE (June 2015)*, http://opensignal.com/reports/2015/05/state-of-lte-q2-2015/ (accessed 9 September 2015).

Optus 2012, *Optus accelerates 3G and 4G expansion via extended site sharing arrangement*, Media Release, 3 May, https://media.optus.com.au/media-releases/2012/optus-accelerates-3g-and-4g-expansion-via-extended-site-sharing-arrangement/ (accessed 9 September 2015).

P3 Communications and TCCA (TETRA + Critical Communications Association) 2015, *Study on the Relative Merits of TETRA, LTE and other Broadband Technologies for Critical Communications Markets*, Aachen, Germany.

PA Consulting Group 2013, *LTE Brings a New Capability to Mobility: How Might it Enable a Range of Cross-Sector Services?*, Report to Ofcom, London.

Paredes, D. 2014a, *Mission Critical ICT at St John NZ*, CIO, www.cio.co.nz/article/557698/mission-critical-ict-st-john-nz/ (accessed 28 August 2015).

—— 2014b, *What corporates can learn from the NZ Police on 'user focus'*, CIO, www.cio.co.nz/article/562347/what-corporates-can-learn-from-nz-police-user-focus/ (accessed 28 August 2015).

PC (Productivity Commission) 2002, *Radiocommunications*, Report no. 22, Canberra.

—— 2011, *Australia's Urban Water Sector*, Report no. 55, Canberra.

—— 2012, *Barriers to Effective Climate Change Adaptation*, Report no. 59, Canberra.

—— 2014a, *Natural Disaster Funding Arrangements*, Inquiry Report no. 74, Canberra.

—— 2014b, *Public Infrastructure*, Inquiry Report no. 71, Canberra.

Penn, A. 2015, 'Telstra CEO Speech: Connecting with the future', www.telstra.com.au/uberprod/groups/webcontent/@corporate/@about/documents/document/uberstaging_295733.pdf (accessed 9 September 2015).

PJCLE (Parliamentary Joint Committee on Law Enforcement) 2013, *Spectrum for Public Safety Mobile Broadband*, Parliament of Australia, Canberra.

Plum Consulting 2008, *Administrative Incentive Pricing of Radiofrequency Spectrum*, London.

PSBA (Public Safety Business Agency) 2014, *Annual Report 2013–2014*, Queensland Government, Brisbane.

—— 2015, *About PSBA*, www.psba.qld.gov.au/about/Pages/default.aspx (accessed 9 September 2015).

Public Safety Canada 2012, *Governance Model for a 700 Megahertz Broadband Interoperable Network for Public Safety in Canada: Workshop Results*, Montreal.

—— 2013, 'Nationwide 700 Megahertz (MHz) Interoperable Public Safety Mobile Broadband Network', presented at Federation of Canadian Municipalities Annual Conference, Vancouver, May.

QFCI (Queensland Floods Commission of Inquiry) 2012, *Queensland Floods Commission of Inquiry*, Final Report, Brisbane.

Queensland Treasury 2015, *Government Wireless Network*, https://treasury.qld.gov.au/projects-infrastructure/projects/government-wireless-network/index.php (accessed 1 September 2015).

RadioReference 2015, *Trunking Basics*, http://wiki.radioreference.com/index.php/Trunking_Basics (accessed 9 September 2015).

Roberson and Associates 2011, *Public Safety Priority Access to Shared Commercial Networks*, Chicago.

SCF Associates 2014, *Is Commercial Cellular Suitable for Mission Critical Broadband?*, Report for the European Commission, Luxembourg.

SCRGSP (Steering Committee for the Review of Government Service Provision) 2014, *Report on Government Services 2014*, Productivity Commission, Canberra.

—— 2015, *Report on Government Services 2015*, Productivity Commission, Canberra.

Shipley, G. 2013, 'UK Emergency Services Mobile Communications Programme (ESMCP)', presented at PSCR Public Safety Broadband Stakeholder Conference, Westminster, Colorado, United States.

—— 2015, 'Emergency Services Mobile Communications Programme', presented at PSCR 2015 Public Safety Broadband Stakeholder Meeting, San Diego.

Shrestha, P.P., Burns, L.A. and Shields, D.R. 2013, 'Magnitude of Construction Cost and Schedule Overruns in Public Work Projects', *Journal of Construction Engineering*, vol. 2013, www.hindawi.com/journals/jcen/2013/935978/ (accessed 20 July 2015).

Simpson, C. 2014, 'The average (theoretical) speed of the FTTN NBN so far is 46Mbps', *Gizmodo*, 8 July, www.gizmodo.com.au/2014/07/average-theoretical-speed-fttn-nbn-46mbps/ (accessed 9 September 2015).

Skinner, T. 2015, 'O2 out of UK Emergency Services LTE Tender, EE Lone Runner', *Telecoms.com*, http://telecoms.com/424831/o2-out-of-uk-emergency-services-lte-tender-ee-lone-runner/ (accessed 28 August 2015).

Smura, T. 2012, 'Techno-economic modelling of wireless network and industry architectures', Aalto University School of Electrical Engineering, Espoo, Finland.

Solomon, H. 2015, *Spectrum: First Responders Wireless Network Inches Forward*, Cartt.ca, https://cartt.ca/article/spectrum-first-responders-wireless-network-inches-forward (accessed 12 August 2015).

Sydney Morning Herald 2014, 'OpenSignal's analysis of Sydney and Melbourne 3G and 4G mobile broadband speeds', Sydney, 24 January, www.smh.com.au/digital-life/mobiles/opensignals-analysis-of-sydney-and-melbourne-3g-and-4g-mobile-broadband-speeds-20140123-31chv.html (accessed 9 September 2015).

Tasmanian Auditor-General 2014, *Report of the Auditor-General No. 10 of 2013-14: Government Radio Communications*, Report no. 10 of 2013-14, Hobart.

TCCA (TETRA + Critical Communication Association) 2013a, *The Strategic Case for Mission Critical Mobile Broadband*, Version 1.0, Newcastle upon Tyne.

—— 2013b, *How to Source a Mission Critical Service*, Newcastle upon Tyne.

Telco Antennas 2014, *2G, 3G, Next-G, 4G: What's the Difference?*, https://www.telcoantennas.com.au/site/guide-to-mobile-networks (accessed 28 August 2015).

Telstra 2011a, *Public Safety and Security: Emergency-Grade Mobile Broadband for the Public Safety and Security Sector*, White Paper, Melbourne.

—— 2011b, *Telstra Annual Report 2011*, Melbourne.

—— 2014a, *Telstra and Motorola Solutions develop public safety broadband solutions*, Media Release, 30 October, www.telstra.com.au/aboutus/media/media-releases/telstra-and-motorola-solutions-develop-public-safety-broadband-solutions.xml (accessed 28 August 2015).

—— 2014b, *Telstra Annual Report 2014*, Melbourne.

—— 2015a, *Telstra Annual Report 2015*, Melbourne.

—— 2015b, *Telstra Case Study: Ambulance Service of NSW*, Sydney.

—— 2015c, *VPN*, https://www.telstra.com.au/business-enterprise/solutions/network-services/networks/vpn (accessed 9 September 2015).

TETRA Applications 2012, 'ASTRID will use 3G network for Mobile Data', http://tetra-applications.com/19596/news/astrid-will-use-3g-network-for-mobile-data (accessed 29 July 2015).

TETRA MoU Association 2004, *Push To Talk over Cellular (PoC) and Professional Mobile Radio (PMR)*, Newcastle upon Tyne.

TETRA Today 2014, 'ASTRID Launches Blue Light Mobile Broadband Data Service', 30 April, www.tetratoday.com/news/astrid-launches-blue-light-mobile-broadband-data-service (accessed 28 August 2015).

The Drum 2010, *Digital Radio Project*, The Drum, www.pfes.nt.gov.au/~/media/Files/Forms_Licences_Permits_Publications/Triservice/Drum_magazine/drum-december-2010.ashx (accessed 9 September 2015).

Transport for NSW 2012, *North West Rail Link Industry Briefing*, NSW Government, Sydney.

Turnbull, M. (Minister for Communications) 2015, *Mobile black spot programme to deliver almost 500 new or upgraded base stations with total investment of $385 million*, Media Release, 25 June, Australian Government, Canberra.

—— and Fletcher, P. (Parliamentary Secretary to the Minister for Communications) 2015, *Next stage of spectrum reform to commence*, Media Release, 25 August, Australian Government, Canberra.

—— and Keenan, M. (Minister for Justice) 2014, *Productivity Commission to make recommendations on mobile broadband for emergency response agencies*, Media Release, 21 November, Australian Government, Canberra.

UK Home Office 2014, *United Kingdom-London: Telecommunications Services, 2014/S 077-133654 Contract Notice*, Tenders Electronic Daily, http://ted.europa.eu/udl?uri=TED:NOTICE:133654-2014:TEXT:EN:HTML&src=0 (accessed 9 September 2015).

—— 2015a, *Eight Organisations Go Forward to Next Stage of Bidding to Run New Network*, https://www.gov.uk/government/publications/the-emergency-services-mobile-communications-programme/eight-organisations-go-forward-to-next-stage-of-bidding-to-run-new-network (accessed 28 August 2015).

—— 2015b, *Emergency Services Mobile Communications Programme*, www.gov.uk/government/publications/the-emergency-services-mobile-communications-programme (accessed 28 August 2015).

UKNAO (United Kingdom National Audit Office) 2002, *Public Private Partnerships: Airwave UK*, London.

—— 2012, *Mobile Technology in Policing*, London.

US Department of Homeland Security 2013, *Interoperability Continuum*, Washington DC.

USGAO (United States Government Accountability Office) 2015, *Public-Safety Broadband Network: FirstNet Should Strengthen Internal Controls and Evaluate Lessons Learned*, GAO-15-407, Washington DC.

VBRC (2009 Victorian Bushfires Royal Commission) 2010, *Final Report*, Melbourne.

VDTF (Victorian Department of Treasury and Finance) 2013, *Procurement Strategy Guideline*, Investment Lifecycle and High Value/High Risk Guidelines, Melbourne.

—— 2015a, *Metropolitan Mobile Radio*, www.dtf.vic.gov.au/Infrastructure-Delivery/Public-private-partnerships/Projects/Metropolitan-Mobile-Radio (accessed 9 September 2015).

—— 2015b, *Mobile Data Network*, www.dtf.vic.gov.au/Infrastructure-Delivery/Public-private-partnerships/Projects/Mobile-Data-Network (accessed 9 September 2015).

Victoria Police 2014, *Victoria Police Blue Paper: A Vision for Victoria Police in 2025*, Victoria.

—— 2015, *About Victoria Police*, www.police.vic.gov.au/content.asp?Document_ID=781 (accessed 24 June 2015).

Victorian Auditor-General 2014, *Emergency Response ICT Systems*, Victoria.

Victorian Department of Justice 2010, *A Layman's Guide to Radio Communications*, Melbourne.

Victorian Government Solicitor's Office 2015, *National Phone Warning System Upgrade Procurement*, www.vgso.vic.gov.au/sites/default/files/Media%20Release.pdf (accessed 3 August 2015).

Vinkvist, J., Pesonen, T. and Peltola, M. 2014, 'Finland's 5 steps to critical broadband', *RadioResource International*, Quarter 4.

Vodafone 2013, *Vodafone to Mobilise New Zealand Police with Smart Technology*, Media Release, 8 March, https://enterprise.vodafone.com/insight_news/2013-03-08-vodafone-to-mobilise-new-zealand-police-with-smart-technology.jsp (accessed 28 August 2015).

WA Department of Commerce 2014, *Regional Mobile Communications Project Overview*, www.commerce.wa.gov.au/industry-and-innovation/regional-mobile-communications-project-overview (accessed 28 August 2015).

Weiss, D. 2015, 'PSMB is not the end state', *Critical Comms*, www.radiocomms.com.au/content/industry/article/psmb-is-not-the-end-state-1162996806 (accessed 9 September 2015).

Wendelken, S. 2014, 'Mission critical PTT set for LTE release 13, release 12 freeze likely in 2015', *Mission Critical Communications*, www.radioresourcemag.com/Features/FeaturesDetails/FID/477 (accessed 15 September 2015).

Woodhouse, M. (Minister of Police and Workplace Relations and Safety) 2014, *New Technology Centre to Help Foster Innovation*, Media Release, 8 December, https://www.national.org.nz/news/news/media-releases/detail/2014/12/08/new-technology-centre-to-help-foster-innovation (accessed 28 August 2015).

World Radiocommunication Conference 2003, *Resolution 646: Public Protection and Disaster Relief*, Geneva.

—— 2012, *Resolution 648: Studies to Support Broadband Public Protection and Disaster Relief*, Geneva.

WYFRA (West Yorkshire Fire & Rescue Authority) 2013, *Emergency Services Mobile Communicaitons Programme*, Birkenshaw, United Kingdom.

Zilis, M. 2014, 'South Korea Plans for Dedicated LTE Public-Safety Network by 2017', *Mission Critical Communications*, www.radioresourcemag.com/Features/FeaturesDetails/FID/482 (accessed 15 September 2015).