Australia Public Safety Mobile Broadband (PSMB) High-Level Requirements

Version 1.2
September 1, 2017

Contents

1 Executive Summary

Across Australia, the public safety community responds to routine and emergency situations at a moment's notice, regardless of the severity. These situations occur daily in every city, town and shire in the country or, in other words, inside and outside population centres.

Coordinated response, across agency lines, including multiple disciplines, is necessary to protect the communities and citizens the public safety community is charged to serve.

The response of the public safety community relies on a communications capability. Recognizing that mobile broadband can be a critical tool for public safety agencies (PSAs), the Public Safety Mobile Broadband (PSMB) Functional Working Group (FWG) was established in May 2017 by the Inter-jurisdictional PSMB Senior Officials Committee (SOC). The SOC was convened by the Australian Commonwealth Government to 'progress work towards a nationally interoperable PSMB capability and report to the Council of Australian Governments (COAG) in late-2017'.

In its role, the FWG developed a draft set of National Objectives (see [1]) for Australia's PSMB capability to guide the development of the draft high-level requirements contained in this document.

The purpose of these high-level requirements is to describe what PSAs – the users – expect of a PSMB capability, helping inform industry and stakeholders of the key elements of a PSMB capability that can support PSAs' multimedia communications, including mission-critical multimedia communications (i.e. communications for which there is an immediate need). In contrast to detailed technical requirements, high-level requirements should be understandable by readers without in-depth technical expertise. The high-level requirements draw upon international standards and requirements developed by public safety agencies in other countries in support of the deployment of a PSMB capability, as well as security requirements specific to Australia's Public Safety Agencies.

The resulting list of high-level requirements is shown below

Domain	HLR No.	High-Level requirement
Services	SERV-1	The PSMB capability will support mission-critical and non-mission-critical multimedia services, including, but not limited to voice, video, data, and exchange of geolocation data
Services	SERV-2	The PSMB capability will support real-time and non-real-time multimedia services
Services	SERV-3	The PSMB capability will support multimedia services for both individual (one-to-one) and group (one-to-many) calls
Services	SERV-4	The PSMB capability will support 3GPP's mission-critical push-to-talk (MCPTT)
Services	SERV-5	The PSMB capability will support machine-to-machine (M2M) communications

Domain	HLR No.	High-Level requirement
Services	SERV-6	The PSMB capability will support geo-localisation services, including the ability to geo-locate responders in indoor environments
Services	SERV-7	The PSMB capability will support concurrent transmission and reception of mission-critical multimedia services to/from users
Services	SERV-8	The PSMB capability will allow dispatchers or other authorised personnel to manage multimedia group communications
Services	SERV-9	The PSMB capability will allow a user to send and receive communications to/from multiple sources including distinct groups
Services	SERV-10	Mission-critical services will be supported when users are off network, including support of device-to-device multimedia communications
Services	SERV-11	The PSMB capability will provide multimedia broadcast communications
Services	SERV-12	A PSMB service will provide the ability for an authorised user (e.g., administrator, dispatcher) to initiate a mission-critical multimedia service remotely
Services	SERV-13	Open Application Programming Interfaces (APIs) will be published and standardised to enable the development of applications leveraging the unique functions of the PSMB capability such as Quality of Service (QoS), priority, and pre-emption, as well as user location, presence, and group communications
Services	SERV-14	All features and services will be tested and validated prior to service launch
Services	SERV-15	PSAs will be able to log, timestamp and store multimedia in a secure manner for later retrieval, including for evidentiary procedures.
Services	SERV-16	PSAs will be able to retrieve PSMB session metadata records on a subscriber basis
Coverage	COV-1	PSMB services will be provided across all locations specified by PSAs at PSA-specified grades of service
Coverage	COV-2	The PSMB Coverage within jurisdiction-specified lists of facilities will be available beyond the first-wall, and where required
Coverage	COV-3	The PSMB coverage is expected to expand incrementally over time to those areas currently served by LMR, taking into account existing LMR investment lifecycles and funding availability determined through respective jurisdictions' budget processes
Coverage	COV-4	In major cities, significant regional and remote population centres, and other identified areas, PSMB services will be supported for users utilising handheld or portable devices.

Domain	HLR No.	High-Level requirement
Coverage	COV-5	In regional, remote areas and other identified areas outside significant population centres, PSMB services will primarily be designed to support users utilising vehicle-mounted devices. Users utilising handheld or portable devices will also have access to PSMB services through a vehicular gateway device.
Coverage	COV-6	In the event of an incident in an area with no PSMB service, transportable or airborne deployable communications assets will be (made) available to provide PSMB services.
Coverage	COV-7	Direct device(s)-to-device(s) communications mode will be possible both inside and outside of PSMB coverage areas
Coverage	COV-8	PSMB services will be supported over air-to-ground links, where airborne assets include helicopters and drones.
Coverage	COV-9	The PSMB coverage will be validated using industry best practices, including operational testing
Coverage	COV-10	Jurisdiction-listed high-risk areas will not lie within the lower percentile of coverage reliability
Coverage	COV-11	PSAs will be provided with up-to-date coverage maps showing the availability of PSMB service, with the expected performance level, in their jurisdictions, as well nationwide maps
Coverage	COV-12	Realtime and non-real-time reporting mechanisms will be available to PSAs to report coverage discrepancies for corrective action by the PSMB service provider
Coverage	COV-13	PSAs will be provided with a periodic PSMB Key Performance Indicators report as determined by their respective business needs
Priority	PRIO-1	In a shared network, access controls will be available to ensure public safety users' applications and devices are given priority service
Priority	PRIO-2	In a congested shared network, access priority given to PSMB users will not impede non-public safety users from initiating emergency calls
Priority	PRIO-3	In a shared network, public safety users will have priority in the assignment and scheduling of PSMB resources.
Priority	PRIO-4	For effective incident response management, the PSMB service will enable designated, and authorised, PSA officials to identify individual public safety personnel and their talk-group affiliations, and determine their device(s) capabilities, and geo-location
Priority	PRIO-5	Quality of service settings will allow for prioritisation of traffic according to the severity of the incident, user type and role, and type of service
Priority	PRIO-6	The PSMB service will enable designated, and authorised PSA officials to dynamically adjust quality of service settings for an individual or group

Domain	HLR No.	High-Level requirement
Priority	PRIO-7	The quality of service for a PSMB multimedia session will be maintained when a public safety device hands off to another PSMB site or another PSMB band, on the same network
Priority	PRIO-8	The quality of service should be maintained when a public safety device roams to another operator's network
Priority	PRIO-9	The PSMB capability will allow for the pre-emption of users or services
Priority	PRIO-10	Public safety emergency calls, including duress calls, will take precedence over other PSMB services
Capacity	CAPA-1	The PSMB capacity will support public safety traffic surges over a given area.
Capacity	CAPA-2	PSAs will have the ability to monitor (on demand) performance metrics for the network, including the number of PS users served at a cell
Capacity	CAPA-3	The PSMB capability will support queuing of multimedia requests
Capacity	CAPA-4	When needed, at the scene of an incident or for a planned PSA activity, additional PSMB resources will be deployed to enhance the PSMB capacity
Capacity	CAPA-5	The deployment of a temporary site to provide PSMB services, at the scene of an incident or for a planned PSA activity, will require minimal human intervention
Capacity	CAPA-6	When the PSMB service is offered by a commercial operator, handoff to other spectrum bands served by the same operator will be possible
Capacity	CAPA-7	When the PSMB service is offered by a commercial operator, roaming onto another commercial operator’s network should be possible where these arrangements exist
Capacity	CAPA-8	PSAs will have access to traffic statistic reports highlighting daily PSMB capacity consumption by public safety users
Capacity	CAPA-9	When needed, designated, and authorised, PSA officials will have the ability to dynamically control quality of service settings for public safety users
Capacity	CAPA-10	Quality of service control will be dynamically performable either from the scene of an incident, or remotely from an emergency/operations/dispatch centre.
Capacity	CAPA-11	In the area of an incident, it will be possible to apply quality of service control while differentiating between the public safety users who are involved in the response and those who are not
Availability	AVAIL-1	Scheduled PSMB maintenance activities will not impede PSMB services
Availability	AVAIL-2	PSMB network facilities will be hardened per existing regulations and/or best engineering practices

Domain	HLR No.	High-Level requirement
Availability	AVAIL-3	The PSMB capability will have appropriate resiliency/redundancy to prevent loss of service.
Availability	AVAIL-4	PSMB radio sites should be capable of operating in an isolated mode
Availability	AVAIL-5	The automatic (and successful) switchover to a backup unit, following the failure of a critical communications network element, will have minimal impact on the PSMB service
Availability	AVAIL-6	The PSMB service will be guaranteed after a switch-over from a failed unit to a standby unit
Availability	AVAIL-7	For each state/territory, the system availability of the PSMB service, in each jurisdiction, will be equivalent to, or better than, the current availability of the jurisdiction's LMR systems
Availability	AVAIL-8	Upon the detection of a partial radio outage, transportable or deployable backup facilities will be available to maintain continuity of the PSMB service
Availability	AVAIL-9	Hardening will be required at sites that serve jurisdiction-listed high-risk areas (e.g, sites which serve large public gatherings, and critical infrastructure)
Availability	AVAIL-10	PSAs will be informed of planned and unplanned outages which impact PSMB services in their jurisdictional area as soon as practicable
Availability	AVAIL-11	PSAs will have access to on-demand service availability reports describing outage periods which affected their jurisdictions and the respective causes
Availability	AVAIL-12	PSAs will have access to monthly service availability reports describing outage periods which affected their jurisdictions and the respective causes
Availability	AVAIL-14	There will be a business continuity and disaster recovery plan per jurisdiction which will be updated on a yearly basis
Security	SECU-1	Sites delivering PSMB services will be protected from unauthorised physical access and equipment tampering
Security	SECU-2	Only PSA-authorised and authenticated personnel will have access to communications facilities supporting PSMB services
Security	SECU-3	Access to fixed telecommunications facilities, and deployables, that provide PSMB services will be accredited by a PSA-designated authority
Security	SECU-4	When using shared resources, public safety traffic should be logically or physically segregated from non-public safety traffic
Security	SECU-5	The integrity and confidentiality of PSMB traffic will be ensured as it propagates through the network, including transit over public network segments

Domain	HLR No.	High-Level requirement
Security	SECU-6	Mobile Virtual Private Networking will be supported
Security	SECU-7	The geo-location of public safety users' will be treated as confidential information and only accessible to PSA-authorised individuals
Security	SECU-8	The end-to-end security of PSMB services and traffic will apply both when communicating on-network (infrastructure mode) and off-network (device-to-device)
Security	SECU-9	The PSMB will ensure that over-the-air exchange of cryptographic keys are confidentiality-protected, integrity-protected and authenticated when delivered over the air
Security	SECU-10	Only PSA-authorised and authenticated users will have access to mission-critical PSMB services and features
Security	SECU-11	The network providing PSMB services will have the appropriate levels of protection against cyber incidents
Security	SECU-12	PSA-authorised users will have the ability to actively monitor all connected users within their jurisdiction at any time
Security	SECU-13	PSAs will be informed of suspicious activities, including suspected malicious attempts as soon as is practicable
Security	SECU-14	Public safety agencies will be informed as soon as practicable of newly detected security vulnerabilities
Security	SECU-15	Security vulnerabilities will be mitigated as soon as practicable
Security	SECU-16	PSMB devices will be validated per agency policies before being allowed access to the network and/or services
Security	SECU-17	For PSMB services contracted from a third-party service provider, third-party service providers will comply with specified requirements of the Protective Security Policy Framework and any other specified protective security protocols
Security	SECU-18	The transfer of information between a PSA and the web (business) portal will be secured
Interoperability	INTEROP-1	The PSMB service should support the ability for a public safety user, away from their home jurisdiction, to access (home or visited) PSMB services in the visited jurisdiction
Interoperability	INTEROP-2	The PSMB service will support the ability for a visitor away from their home jurisdiction, to join a group in the visited jurisdiction
Interoperability	INTEROP-3	Both uplink and downlink seamless mobility will be supported as a public safety user 'roams' from one jurisdiction to another
Interoperability	INTEROP-4	Services should be tested across jurisdictions prior to deployment to ensure they don't adversely affect interoperability

Domain	HLR No.	High-Level requirement
Interoperability	INTEROP-5	To maintain service interoperability across jurisdictions, network upgrades (including the introduction of new features) will not compromise interoperability
Devices	DEV-1	PSMB devices will include form factors such as handhelds, vehicular modems, tablets, wearables and machines, and associated accessories
Devices	DEV-2	PSMB devices for airborne and maritime operations will be supported
Devices	DEV-3	PSMB devices which support device-to-device communications will be made available to PSAs
Devices	DEV-4	Public-safety-grade devices should include units which support both existing LMR and LTE services
Devices	DEV-5	The PSMB device will allow sharing by multiple users, each with their own profile
Devices	DEV-6	The PSMB service will support the concurrent use of multiple devices by a single user
Devices	DEV-7	Supported PSMB devices will be comprised of both consumer-grade and public safety-grade devices
Devices	DEV-8	Ruggedised/Public safety-grade devices will be suitable for use in the environments and circumstances public safety users operate in. Specifications for these devices will include consideration of appropriate battery life, protection against dust, humidity, shock, heat and vibration.
Devices	DEV-9	Public safety agencies will have the ability to remotely provision, configure, disable, and erase the contents of (wipe) supported devices
Devices	DEV-10	Authorised BYODs (“Bring Your Own” Devices) will be provided with access to PSMB services
Devices	DEV-11	All PSMB devices will be type-approved by a PSA-designated entity
Devices	DEV-12	Any new features added to the PSMB capability will be added in a way that ensures all PSMB devices are backwardly compatible
Devices	DEV-13	For remote and any unserved PSMB areas, PSMB devices should include units capable of both terrestrial PSMB access and satellite access
Integration	INTEG-1	A public safety user using the LMR service and a public safety user using the PSMB service will be able to communicate with each other
Integration	INTEG-2	Dispatchers will be able to monitor and communicate simultaneously with both LMR and PSMB users via a console
Integration	INTEG-3	LMR to LTE interworking operations will comply with 3GPP standards
Integration	INTEG-4	When audio propagates from LTE to LMR, or vice versa, any transcoding will not adversely impair the quality of the communications

Domain	HLR No.	High-Level requirement
Integration	INTEG-5	Group communications between PSMB talk-groups and LMR talk-groups will be supported
Integration	INTEG-6	End-to-end secure communications between a LMR user/console and a LTE user, or between a LMR talk-group and a LTE talk-group will be supported
Standards	STAND-1	The PSMB service will, at a minimum, use 3GPP Release 13 for baseline specifications
Standards	STAND-2	The PSMB service will support standard mission-critical quality of service (QoS) parameters
Standards	STAND-3	The PSMB service will support standard prioritisation including the ability to preempt services
Standards	STAND-4	PSMB devices will be 3GPP standards compliant
Standards	STAND-5	Mission-critical applications will comply with existing standards as much as practically feasible
Standards	STAND-6	The PSMB network external interfaces will be standards compliant
Standards	STAND-7	The PSMB capability will benefit from latest advances in standards specifications, when applicable.
Standards	STAND-8	PSAs will be provided with the process and roadmap associated with the implementation of standardised mission-critical feature sets

Table 1 High-Level Requirements

The draft high-level requirements of Table 1 purposely do not identity *how* such a public-safety capability might be delivered: the requirements are applicable whether the PSMB capability is delivered via commercial operators' networks, networks dedicated to public safety, or hybrids of these approaches. The high-level requirements specify *what* the solutions should be designed to achieve rather than *how* the solutions should be designed to achieve the requirements. Since no time frame is considered for the availability of a particular capability, the requirements described herein represent the desired end-state of a PSMB capability which is consistent with achieving the national objectives.

While the draft high-level requirements cover what is desired from a functionality perspective, the FWG has opted to include a number of quantitative performance requirements to illustrate the important distinction between mission-critical and non-mission-critical services[1]. These performance-

[1] The standardization body 3GPP defines Mission Critical as follows: Quality or characteristic of a communication activity, application, service or device, that requires low setup and transfer latency, high availability and reliability, ability to handle large numbers of users and devices, strong security and priority and pre-emption handling. See [2]

69 based requirements are listed in the following Table[2]. Descriptions and additional detail is provided
70 in the Appendix.

PR No.	Performance Requirement
PR-1	The PSMB portable service bandwidth should be characterised by a minimum uplink (device to network) user throughput of 256 kbps and minimum downlink (network to device) throughput of 768 kbps
PR-2	The PSMB vehicular service bandwidth on major and secondary roads should achieve a minimum uplink user throughput of 1 Mbps and minimum downlink throughput of 1 Mbps
PR-3	The PSMB vehicular service bandwidth in remote areas, except for major and secondary roads (as covered in COV-8), should achieve a minimum user throughput of 64 kbps on the uplink and 256 kbps on the downlink
PR-4	The PSMB maritime service bandwidth should achieve a minimum user throughput of 1 Mbps on the uplink and 1 Mbps on the downlink
PR-5	The PSMB service should provide portable indoor coverage within PSA-designated facilities with at least 95% reliability
PR-6	The PSMB service should provide portable outdoor coverage in major cities and regional towns with at least 97% reliability
PR-7	The PSMB service should provide portable outdoor coverage in and around jurisdiction-listed major risk areas with at least 97% reliability
PR-8	The PSMB service should provide mobile coverage along roads and railroads with at least 95% reliability
PR-9	The PSMB service should provide mobile coverage in rivers, lakes and coastal areas with at least 95% reliability
PR-10	For areas not covered by PR-5 to PR-9, the PSMB service should provide mobile coverage with at least 95% reliability
PR-11	The retainability rate of PSMB services should be at least 99%
PR-12	The accessibility rate of PSMB services should be at least 99%
PR-13	The success rate of handover of sessions should be at least 99%
PR-14	Radio coverage maps will have a resolution of 30m by 30m, or better
PR-15	The service availability, on a jurisdiction basis, should be at least 99.99% as a monthly average

[2] There is an expectation that a more complete set of detailed technical requirements would follow the development of these high-level requirements. The Recommendations are likely to become technical requirements or specifications.

PR No.	Performance Requirement
PR-16	The average time to restore the PSMB service should be no more than 4 hours in metropolitan areas, 6 hours in regional areas, and 8 hours in remote areas
PR-17	Historical PSMB service availability data describing outage periods and the respective causes should be stored for a period of at least 10 years

71 *Table 2 Performance Requirements*

72

73 2 High-Level Requirements

74 2.1 Introduction

75 The PSMB National Objectives [1] developed and endorsed by the FWG are listed below.

Objective No.	Objective
0	Australian Governments will work co-operatively to develop a federated Public Safety Mobile Broadband Capability (PSMB) in Australia, that takes account of individual jurisdictional circumstances
1	Services - Australia's PSMB capability will support the provision of both mission-critical and non-mission-critical multimedia services
2	Coverage - Australia's PSMB capability will provide, as far as is feasible, coverage that is fit-for-purpose for PSAs
3	Priority - Australia's PSMB capability will be able to prioritise between different PSA users, and, where the use case requires it, provide priority access to PSA's when service resources are shared with non-public safety users
4	Capacity - Australia's PSMB capability will be scalable to accommodate public safety needs
5	Availability - Australia's PSMB capability will, as far as is feasible, be available at all times
6	Security - Australia's PSMB capability will have appropriate protective security measures to prevent unauthorised access of information and interference.
7	Interoperability - Australia's PSMB capability will provide nationwide interoperable public safety communications, including communications within and between jurisdictions
8	Devices - Australia's PSMB capability will be accessible on any fit-for-purpose device across multiple operating systems
9	Integration - Australia's PSMB capability will complement and, where appropriate, be integrated with jurisdictional land mobile radio capabilities.
10	Standards - Australia's PSMB capability will be based on open standards, with any proprietary features of the capability reverting to a standardised version once available

This section outlines the high-level requirements associated with objectives 1-10 above. (We note that objective 0 is a non-technical objective, and therefore will not have associated high-level technical requirements.) To give the reader context, a short description of the FWG's rationale precedes each requirement. Emphasis has been placed on presenting mandatory requirements for the PSMB capability. The word 'will' is used to declare the mandatory nature of a requirement. 'Should' is used to declare those requirements that are desired from the PSMB capability. Requirements using the word 'should' are not mandatory.

The order the high-level requirements are listed in this document is arbitrary. Hence, no prioritization among the requirements is implied by the order in which they appear. For better readability, footnotes are used for additional clarification, when needed.

2.2 Services[3]

Multimedia services will be used to support PSA operations in a variety of ways. Much of this use will be mission-critical: for example, conversing over push-to-talk while livestreaming of video from helmet- and body cams during an incident. PSAs also require mission-critical data services including situational awareness, Computer Aided Dispatch, geo-location, monitoring of body-worn sensors to assess the health of PSA personnel, control of robots, aid in decision-making, etc. Some multimedia use by PSAs will be non-mission-critical: for example, a unit-to-unit voice call, email, web access to agency intranet sites, or instant messaging to accomplish an administrative task.

SERV-1 The PSMB capability will support mission-critical and non-mission-critical multimedia services, including, but not limited to voice, video, data, and exchange of geolocation data

Real-time video is a critical tool for providing situational awareness. Examples include the delivery of live video streams from dashboard cameras to dispatchers or an incident command centre during an incident. Some of the multimedia used to support PSA operations will be exchanged in non-real-time (e.g., the delivery of a public safety device software update over the PSMB service).

SERV-2 The PSMB capability will support real-time and non-real-time multimedia services.

[3] The term Multimedia is used to describe next generation PSMB services including voice services.
Mission Critical Applications: Generic communication applications with mission critical characteristics, traditionally encompassing push-to-talk voice (MCPTT), real-time video (MCVideo) and real-time data (MCData). See 3GPP specifications at [2].
The term Service should be understood herein as a communications service. An application is typically a service enabler.

Public safety operations require communication among members of teams, between teams, and between individuals. Team-based communication among teams comprised of 3 or more members is referred to as one-to-many communications. One-to-many communication – where one member of the team sends multimedia and the rest of the team receive it – is an essential tool for coordinating teams during day-to-day, incident, planned event operations and disaster management. Communications between two devices is known as one-to-one communications. One-to-one communication is also an essential tool for private communications between individual first responders.

SERV-3 The PSMB capability will support multimedia services for both individual (one-to-one) and group (one-to-many) calls

Section 4.2 gives a background on mission-critical push-to-talk (MCPTT) service, the voice service used by public safety to support public safety operations, and how MCPTT differs from the push-to-talk services offered by commercial service providers today. 3GPP, the body that develops standards for the Long Term Evolution (LTE) technology that will be used by the PSMB service, is developing an extensive set of features for support of MCPTT. 3GPP's MCPTT features define a push-to-talk service comparable in performance, scalability, and functionality to today's public safety Land Mobile Radio push-to-talk service. The following requirement reflects PSA's needs for support of MCPTT over the PSMB capability.

SERV-4 The PSMB capability will support 3GPP's mission-critical push-to-talk (MCPTT)

The following requirement covers machine-type communication, such as drone-to-drone or sensor-to-server communications (e.g., from a field camera to a video management server, heat or smoke sensors direct to turnout systems).

SERV-5 The PSMB capability will support machine-to-machine (M2M) communications

Regular reporting of geolocation data is essential to help ensure the safety of public safety personnel. In addition, such information helps decrease incident response times (through Computer Aided Dispatch, for example). Current technologies are capable of estimating the location of a device in 2 dimensions. Since public safety responders also operate in multi-story buildings, it is desirable that this capability evolve to provide 3-dimensional position estimates once this technology is readily available.

SERV-6 The PSMB capability will support geo-localisation services, including the ability to geo-locate responders in indoor environments

The following requirement reflects the needs of public safety responders to have simultaneous access to multiple sources of information to coordinate operations. For example, public safety responders will engage in a 2-way audio/video conversation while sharing maps or images.

SERV-7 The PSMB capability will support concurrent transmission and reception of mission-critical multimedia services to/from users and resources

The following requirement is designed to help manage multimedia communications. Such functionality is required, for example, to allow a dispatcher to select a video feed and deliver the video feed to a selected group. This function is analogous to the patching of (voice) talk-groups in today's Land Mobile Radio networks.

SERV-8 The PSMB capability will allow dispatchers or other authorised personnel to manage multimedia group communications

The following requirement reflects the need for an incident commander, for example, to send and receive multimedia to/from different groups.

SERV-9 The PSMB capability will allow a user to send and receive communications to/from multiple sources including distinct groups

The following requirement reflects the need to support off-network multimedia services when within or outside the coverage area of the PSMB network. This will be accomplished through LTE's device-to-device communications mode.[4]

SERV-10 Mission-critical services will be supported when users are off network, including support of device-to-device multimedia communications

The following requirement distinguishes broadcast calls from group calls. In contrast to group calls, data delivered via broadcast is delivered without expecting a response from the recipients. One example of a broadcast call is messages originating from a tsunami early warning system and sent to all public safety personnel.

SERV-11 The PSMB capability will provide multimedia broadcast communications

[4] In LMR voice systems this is referred to as talk-around or Direct Mode Operation. Switching to such a communications mode in today's LMR systems is typically done manually. It can take place within the coverage footprint of a site.

Using Project 25 digital radio (P25) Remote Unit Monitoring feature, a dispatcher can trigger an audio session without intervention from the device's user. This feature is useful in hostage situations, for example, as it allows a dispatcher to discreetly hear what is happening. With PSMB, this feature can be extended to collect video streams from a user's body camera, for example.

SERV-12 A PSMB service will provide the ability for an authorised user (e.g., administrator, dispatcher) to initiate a mission-critical multimedia service remotely

Use of Open Application Programming Interfaces to access PSMB functions will allow PSAs to procure applications from a variety of vendors, as well as develop their own applications.

SERV-13 Open Application Programming Interfaces (APIs) will be published and standardised to enable the development of applications leveraging the unique functions of the PSMB capability such as Quality of Service (QoS), priority, and pre-emption, as well as user location, presence, and group communications

Services or features must be thoroughly tested and validated prior to being launched. Failure to do so increases the risks public safety officials face during their day-to-day work.

SERV-14 All features and services will be tested and validated prior to service launch

Logging and recording of audio is standard practice in public safety operations, and a required feature of public safety Land Mobile Radio systems. This capability must be extended to also support the logging of video and data.

SERV-15 PSAs will be able to log, timestamp and store multimedia in a secure manner for later retrieval, including for evidentiary procedures.

For incident re-creation and storyline analysis, public safety agencies have a desire to trace PSMB data sessions on a per user basis. Data should be in a form usable by a PSA since this data is often intended for network management and optimization. PSAs may also look at the data for verifying quality of service provided by the PSMB network.

SERV-16 PSAs will be able to retrieve PSMB session metadata records on a subscriber basis

2.3 Coverage

The Australian Bureau of Statistics' (ABS) Remoteness Structure classifies Australian geography using the following classes: Major city, Inner regional, Outer Regional, Remote and Very Remote [3].

For the purpose of developing the HLR, we use three high level-classifications of Australian geography: Metropolitan, Regional and Remote. The mapping of these three classifications to ABS's Remoteness Structure classes is as follows:

PSMB HLR Classification	Corresponding Australian Bureau of Statistics Remoteness Structure Class(es)
Metropolitan	Major City
Regional	Inner Regional, Outer Regional
Remote	Remote, Very Remote

First-responders operate across a variety of environments (e.g., metropolitan, regional, remote, maritime, coastal regions, lakes, rivers), in different physical circumstances (indoor, outdoor, underground, at sea, in the air), in hostile environments (fires, chemical incidents, explosive conditions), and for different operational situations (e.g., day-to-day, planned events and incident response)[5]. A PSMB capability needs to be able to provide PSAs services where and when they need them. Each jurisdiction will develop its own specific coverage requirements and PSMB coverage is expected to expand incrementally over time to those areas currently served by LMR[6] . Further, PSAs require homogenous service and service continuity across the areas they operate in. Through the minimization of radio coverage holes (i.e., areas where service is unavailable), the capability should provide services with the highest level of coverage reliability and ensure a guarantee of coverage throughout a service area.

COV-1 PSMB services will be provided across all locations specified by PSAs at PSA-specified grades of service

The following requirement pertains to typical public safety operating environments, particularly indoor in metropolitan and regional areas. Jurisdictions will provide lists of facilities where PSMB coverage is required indoors.

Since radio signals weaken when they pass through building walls, it is essential that coverage of the PSMB service in metropolitan and regional areas is designed to reach the inside of facilities specified by public safety officials. These facilities may include tunnels, subway stations, underground structures, and buildings such as manufacturing plants, malls, airports, hospitals, etc[7]. It is customary for Land Mobile Radio systems to be designed to provide coverage beyond the first

[5] See Appendix for the regional classification

[6] Taking into account existing LMR investment lifecycles and funding availability determined through respective jurisdictions' budget processes

[7] This is contingent on local laws and regulations and/or property owners' policies. For instance, in the United States, some jurisdictions do not allow sharing of a neutral Distributed Antenna System host between commercial and public safety services. In other cases, the high hardening costs due to fire codes can be significant disincentives to property owners to deploy such neutral-host solutions.

wall of a building. Some designated sites, such as shopping centres, for example, may be outfitted with distributed antenna systems to ensure adequate radio coverage throughout the facility.

COV-2 The PSMB coverage within jurisdiction-specified lists of facilities will be available beyond the first wall, and where required

The following requirement pertains to the end-state of a migration from legacy LMR services to a PSMB service. The timing of this migration is expected to vary across Australia's states and territories. In addition, there may be a desire to keep legacy LMR operational in remote areas.

COV-3 The PSMB coverage is expected to expand incrementally over time to those areas currently served by LMR, taking into account existing LMR investment lifecycles and funding availability determined through respective jurisdictions' budget processes

The following requirement is designed to ensure delivery of multimedia services to public safety users while they walk or drive at street level in metropolitan and regional service areas.

COV-4 In major cities, significant regional and remote population centres, and other identified areas, PSMB services will be supported for users utilising handheld or portable devices.

The following radio planning requirement is designed to reduce the gap between mission-critical-LTE coverage and LMR footprints in remote areas.

COV-5 In regional, remote and other identified areas outside significant population centres, PSMB services will primarily be designed to support users utilising vehicle-mounted devices. Users utilising handheld or portable devices will also have access to PSMB services through a vehicular gateway device[8].

Incidents can occur outside the planned coverage area of a PSMB service. In such cases, airborne PSMB assets or base stations on wheels will be needed to support public safety operations[9]. These deployable units may require satellite connectivity to link the deployable units with PSA intranets.

COV-6 In the event of an incident in an area with no PSMB service, transportable or airborne deployable communications assets will be (made) available to provide PSMB services.

[8] This requirement does not preclude the possibility of a handheld service. Further, 3GPP specifications include the possibility of a so-called UE-network relay (i.e. similar to the gateway concept).

[9] Deployable assets may consist of a complete standalone LTE system which includes applications servers. In such scenarios, (satellite) backhaul may be or may not be required.
The use of satellite in remote areas to provide PSMB-like services is covered under the Devices section

The following requirement is intended to address the need for tactical communications, e.g. prior to the arrival of a deployable, inside a building, during covert operations, at sea, or in other areas not served by the PSMB network's fixed infrastructure[10].

COV-7 Direct device(s)-to-device(s) communications mode will be possible both inside and outside of PSMB coverage areas.

The following requirement reflects the need for (on-demand) air-to-ground and water-based broadband communications during day-to-day operations[11]. A car chase involving the use of a law enforcement helicopter is such an example. Air-to-ground communications service may require a spectrum band distinct from the terrestrial network[12].

COV-8 PSMB services will be supported over air-to-ground links, where airborne assets include helicopters and drones

The following requirement relates to coverage testing prior to launching the PSMB service or for acceptance purposes.

COV-9 Network coverage will be validated using industry best practices, including operational testing

High-risk areas are areas defined by jurisdictions where it is essential that reliable wireless connectivity is provided (e.g., stadiums and chemical plants, and their surroundings, where Public Safety Agency personnel face higher incidental risk). Coverage reliability tests characterise a percentile X of location areas meeting the grade of service. The following requirement is to ensure that single high-risk areas lie within those location areas (tiles).

COV-10 Jurisdiction-listed high-risk areas will not lie within the lower percentile of coverage reliability

To help plan operations, PSAs must know where to expect PSMB service within their respective jurisdiction. Further, because network operators' may frequently optimise wireless coverage, new coverage maps must be made available as and when changes are made.

[10] In contrast to SERV-10 which speaks about applications, this requirement is to indicate that additional coverage can be achieved via device-device communications without risk of significant interference

[11] The criticality of an air-to-ground solution is more acute in areas served by the terrestrial network because of coverage overlap. In unserved areas, the spectrum band used by the terrestrial network may be leveraged.

[12] The use of the 4.9 GHz is an option. Other countries may follow a different route

COV-11 PSAs will be provided with up-to-date coverage maps showing the availability of PSMB service, with the expected performance level, in their jurisdictions, as well nationwide maps

Coverage map data must be as accurate as possible. Therefore, regular updating of coverage maps based on PSA users' experience, or measurement feedback from PSMB devices to the network, must be provided by the PSMB capability.

COV-12 Realtime and non-real-time reporting mechanisms will be available to PSAs to report coverage discrepancies for corrective action by the PSMB service provider

PSAs need to know how well the PSMB system is performing.

COV-13 PSAs will be provided with a periodic PSMB Key Performance Indicators report as determined by their respective business needs

2.4 Priority

The following requirement is designed to ensure that when public safety users access a congested network, their multimedia traffic is prioritised appropriately[13].

The first hurdle in the process is contention on the so-called random-access channel which enables the device's first communication with the network[14]. The number of network resources associated with this channel is limited. The amount of resources assigned to this random-access channel is based on engineering assumptions on the number of number of devices found in the coverage area of the cell and their activity. Congestion will occur when the rate of such attempts grows beyond the supported capacity of the base station's random-access channel. A number of mechanisms, including controlling the number of retries and using back-off timers, may alleviate the congestion by trying to spread access attempts over time. When those mechanisms are not sufficient, the network begins to bar access to the site using a process known as 'Access class barring." Access class control prevents a fraction of devices from accessing the site based on the access class controls pre-provisioned in the device's USIM card.[15] Access class barring typically targets access classes 0 to 9. Public safety users have a special, reserved access class (AC12) but some lower-priority

[13] Congestion is determined by the network operator/manager since tools will be available at a network operating center. The availability of congestion information to individual PSAs, and what constitutes congestion, is contingent on the terms of Service Level Agreements agreed with the PSMB provider.
[14] The use of the random access channel is not limited to initial registration. For example, it is also used when the device moves from an idle state to a connected state. Also, the standard allows for non-contention on the random access during handovers by reserving a set of pre-determined preamble sequences.
[15] USIM: Universal Subscriber Identity Module.

officials, based on their role and function, may be provisioned with an access class between 0 and 9[16].

Once access to the network is successful, the next hurdle is for the user to be *admitted* and granted a 'bearer'. A bearer is a network radio resource used to carry data – 'bearer traffic' – between the device and the network. At this point, the priority attribute of the public safety user becomes relevant. The capacity of a radio site (or a cell), in terms of number of bearers available, resources blocks available, backhaul bandwidth, or number of connected users, will dictate whether a high priority call gets admitted by, for example, pre-empting a lower priority user.

Once admitted, *scheduling* of network resources to enable a user's session or sessions will account for their priority level, allowed services, QoS, etc. These attributes are contained in the subscriber's profile. The profile also includes an indication whether the user can pre-empt another user or be pre-empted.

The following requirement implies that processes and tools, which interface with the network, will be available to achieve the desired level of control[17].

PRIO-1 In a shared network, access controls will be available to ensure public safety users' applications and devices are given priority service

When a shared network is congested because it cannot handle a storm of access requests, access class barring is a standard mechanism to reject all or a percentage of the access requests. The access class is provisioned in the device's subscriber module. From the perspective of a (barred) user in the footprint of a barred cell, the network is unavailable (i.e., equivalent to the user being in an unserved area).[18] The following requirement is designed to ensure that in a shared network, emergency calls originating from non-public safety users are delivered successfully during periods of congestion. Emergency ('000') calls are assigned a special access class (AC10) to help ensure they are able to be completed during periods of congestion. Further, given that 3GPP standards allow a 'per application' for access class barring, there should be an option to allow only certain types of emergency calls.

PRIO-2 In a congested shared network, access priority given to PSMB users will not impede non-public safety users from initiating emergency calls

[16] When the site is operating in an isolated mode, the 3GPP standard mandates the use of specific access class (11 and 15) for local operations. In that case, the device is expected to be provisioned with a modified USIM or an addiitonal USIM application (see e.g. 3GPP TS 31.102).
[17] See for example, AT&T's plan regarding FirstNet users: "The Incident Management Tool (IMT) will allow agencies to categorize specific users to priority above other users during emergencies. This priority will be temporary and will expire after a given period of time determined by the agency."
[18] Cell barring of all users, including public safety users, may occur if maintenance on a specific site is necessary, e.g. for hardware upgrade, troubleshooting or replacement of faulty hardware.

The following requirement reflects the need for priority services for calls that have already been admitted. This need arises when insufficient radio resources are available to serve a particular service at the quality of service required.

PRIO-3 In a shared network, public safety users will have priority in the assignment and scheduling of PSMB resources.

The following requirement is designed to help the PSA official determine the type of public safety user, their device capabilities and geo-location for more effective control of QoS across the incident area. Normally, this will be managed by the incident's lead agency.

PRIO-4 For effective incident response management, the PSMB service will enable designated, and authorised, PSA officials to identify individual public safety personnel and their talk-group affiliations, and determine their device(s) capabilities, and geo-location

The following requirement is designed to ensure adequate quality of service while favouring communications for critical members of the response team.[19]

PRIO-5 Quality of service settings will allow for prioritisation of traffic according to the severity of the incident, user type and role, and type of service

The following requirement for group QoS reflects the case where, e.g. a hostage situation, all members of a Special Weapons And Tactics (SWAT) Team have high-priority when communicating using mission-critical voice.

PRIO-6 The PSMB service will enable designated, and authorised PSA officials to dynamically adjust quality of service settings for an individual or group

The following requirement will ensure, for instance, that the transmission of a video feed from an ambulance heading towards a hospital while crossing multiple radio footprints of the same network, is received with a consistent quality of service.

PRIO-7 The quality of service for a PSMB multimedia session will be maintained when a public safety device hands off to another PSMB site or another PSMB band, on the same network

[19] User type may include their function and role.

The following requirement reflects the desire that the transmission of a video feed from an ambulance heading towards a hospital while crossing multiple radio footprints, is received with a consistent quality of service. Maintaining priority is contingent on the terms of the roaming arrangement, therefore there is no guarantee that the policy of the visited network will allow such a favourable treatment

PRIO-8 The quality of service should be maintained when a public safety device roams to another operator's network

The following requirement is designed to ensure that during loaded network conditions, PSA users have the ability to run critical PSMB services. To accomplish this, except for in-progress emergency calls, some users' transmissions may need to be pre-empted. Pre-emption may include transmissions of lower-priority public safety users or specific services. While such pre-emption can occur automatically based on rules provisioned in the network traffic policy engine, and the provisioned subscribers' profiles, the ability for designated officials to adjust policy settings is required. This requirement is different from PRIO-1 which is specific to the access phase.

PRIO-9 The PSMB capability will allow for the pre-emption of users or services

This requirement ensures that PSA emergency calls – including duress calls - have the highest priority. 'Duress calls' are issued by first responders who find themselves in perilous situations. Such situations include police officers who have been taken hostage.

PRIO-10 Public safety emergency calls, including duress calls, will take precedence over other PSMB services

2.5 Capacity

Public safety incidents vary in severity and services used in supporting PSA response. As a result, the PSMB traffic load varies; every sq-km2 can become a traffic hot-spot at different times[20]. In general, the number of resources (personnel, equipment and vehicles) brought to an incident location increases according to the incident severity type[21]. The demand generated by the emergency response to an urban multi-dwelling fire can far exceed the demand generated by a

[20] The (additional) demand due to organic public safety traffic growth, is expected to be part of the usual PSMB service capacity planning.
[21] For example, (2013) police metrics from the UK Home Office indicate more than 10 times increase in the number of resources per (TETRA) sector, between a Business-As-Usual event vs. a planned large event.

response to a single car accident[22]. Mechanisms described in the Priority section will be used in that respect. The following requirement would apply to a cell (minimal area), a site or a cluster of sites[23].

CAPA-1 The PSMB capacity will support public safety traffic surges over a given area.

The following requirement is to provide PSAs the ability to monitor key performance indicators.

CAPA-2 PSAs will have the ability to monitor (on demand) performance metrics for the network, including the number of PS users served at a cell

There will be times when the demand for PSMB services exceeds the capacity of the PSMB network. In such cases, it is advantageous to queue requests for service, completing queued calls when network resources become available. For voice over LTE calls, for example, queuing may occur during the call admission process.

CAPA-3 The PSMB capability will support queuing of multimedia requests

The following requirement reflects a situation when an incident takes place, for instance, at the edge of a cell.

CAPA-4 When needed, at the scene of an incident or for a planned PSA activity, additional PSMB resources will be deployed to enhance the PSMB capacity

The following requirement reflects the need to quickly boost the local capacity via minimal adjustments to the network or the capacity relief platform. The ability to rapidly deploy one or more temporary small cells within the larger footprint of a permanent cell, while ensuring interference control, is one example.

CAPA-5 The deployment of a temporary site to provide PSMB services, at the scene of an incident or for a planned PSA activity, will require minimal human intervention

In a shared network, the following requirement relates to the possibility of distributing traffic (off-loading) across available spectrum bands to relieve the congested band.

CAPA-6 When the PSMB service is offered by a commercial operator, handoff to other spectrum bands served by the same operator will be possible

---

[22] ITU refers to those events as PP1 (day-to-day) and PP2 (large events). Disaster relief will apply to larger areas, i.e. encompassing more than one single radio PSMB site.

[23] A traffic surge can be in terms of number of users, aggregate throughput, number of bearers, etc., or essentially, all those parameters whose metrics are constrained by hard or soft capacity limits in the network

In a shared network, the following requirement relates to the possibility of leveraging existing roaming agreements the operator has with peer operators

CAPA-7 When the PSMB service is offered by a commercial operator, roaming onto another commercial operator's network should be possible where these arrangements exist

To better determine future demand, bandwidth needs, and operating procedures, PSAs will need to know their actual traffic demand. Access to a portal will be needed. PSAs, for example, may want to know how much traffic they generate on a periodic basis; this is already the case with commercial wireless service subscriptions.

CAPA-8 PSAs will have access to traffic statistic reports highlighting daily PSMB consumption by public safety users

During incident response, incident commanders, remote dispatchers, or emergency managers must be able to dynamically set priorities, user and application bandwidths to quickly meet the needs of the response[24]. An implicit assumption is that the PSMB provider will provide the means to achieve such control.

CAPA-9 When needed, designated, and authorised, PSA officials will have the ability to dynamically control quality of service settings for public safety users

CAPA-10 Quality of service control will be dynamically performable either from the scene of an incident, or remotely from an emergency/operations/dispatch centre.

The following requirement reflects a situation where, for example, firefighters are battling a fire in an area where a counter terrorism exercise (law enforcement drill) is being conducted. Therefore, preference is given to the incident responders. The area can be served by the same site (or cell).

CAPA-11 In the area of an incident, it will be possible to apply quality of service control while differentiating between the public safety users who are involved in the response and those who are not

[24] Local, and inter-regional, policies will dictate the operating procedures for such a control.

2.6 Availability

The following requirement is designed to ensure that there is minimal service interruption during planned maintenance intervals. Planned software or hardware upgrades need to be scheduled so as not to conflict with public safety operations. It is worthy of mention that the time windows typically used by commercial service providers to upgrade software/hardware (early hours over weekends) may occur during the times public safety incidents are most frequent.

AVAIL-1 Scheduled PSMB maintenance activities will not impede PSMB services

The following requirement is multi-fold as it addresses the need for site hardening through the use of shelters and reinforced structures. These structures protect PSMB base stations and other network infrastructure against human attacks (e.g. vandalism, tampering) and natural events (wind, flooding, fire).[25]

AVAIL-2 PSMB network facilities will be hardened per existing regulations and/or best engineering practices

In addition to natural hazards such as flooding or storms which may cause the destruction of a site, loss of power is one of the primary causes of outages. Battery banks and generators are commonly used to mitigate the risk of power outages.

AVAIL-3 The PSMB capability will have appropriate resiliency/redundancy to prevent loss of service.

The loss of backhaul due to a fibre cut or loss of microwave antennas has led to the introduction of a fail-safe feature in public safety LMR networks. 'Failsafe' is the ability for a radio site to operate in a stand-alone mode. 3GPP has developed similar specifications to enable such mode of operation (Isolated Operation for Public Safety)[26].

AVAIL-4 PSMB radio sites should be capable of operating in an isolated mode

The following requirement is to ensure quick switch-over from a failed circuit pack, or from a failed product, to a redundant unit in standby-mode. The switch-over must be imperceptible to users of the PSMB service.

---

[25] See for example **Error! Reference source not found.** and [12].

[26] It is not clear at this stage, given the large number of sites which will be required to cover a service area, whether all base stations should be capable of operating in stand-alone. The use of fail-safe features in regional or remote sites may be more likely, especially for sites served by a single microwave spur.

AVAIL-5 The automatic (and successful) switchover to a backup unit, following the failure of a critical communications network element, will have minimal impact on the PSMB service

The following operational readiness requirement is designed to ensure that, through monitoring redundant equipment from a network management system, switch-over after failure should ensure service continuity[27]

AVAIL-6 The PSMB service will be guaranteed after a switch-over from a failed unit to a standby unit

Coverage overlap (coverage areas reachable by more than one radio site) may help maintain services in the case of a radio site outage. Metropolitan areas typically have a high density of radio notes. As a result, coverage overlap in metropolitan areas is typically high. In contrast, regional and remote areas have significantly lower densities of radio nodes. As a result, coverage overlap will likely low in regional or remote areas[28]. (Note: whilst devices are critical end-points for service, their failure rate is not usually included in network availability metrics.)

AVAIL-7 For each state/territory, the system availability of the PSMB service, in each jurisdiction, will be equivalent to, or better than, the current availability of the jurisdiction's LMR system systems

When the PSMB service experiences an outage due to loss of radio coverage, it must be quickly restored[29]. There is an expectation that PSAs should be allowed to have their own deployable.

AVAIL-8 Upon the detection of a partial radio outage, transportable or deployable backup facilities will be available to maintain continuity of the PSMB service

'Hardening' refers to the provision of additional backup power, strengthening of antenna structures, and other techniques to mitigate the risk of a network outage. The following requirement addresses the need to harden sites in regions with critical infrastructure (e.g. oil and gas storage facilities, power plants, chemical plants, reservoirs, dams, etc.), areas with large numbers of people (airports, train terminals, etc.) or areas prone to natural hazards (e.g. flooding, wildfires, cyclones).

---

[27] It is sometimes preferable to run units in active-active mode rather than active-standby mode.
[28] For example, RF transmit power settings of the radio sites could be adjusted to help make up for the loss of coverage
[29] Partial outage is referring to a fraction of the radio network. In a dense radio network, e.g. in major cities, the loss of coverage due to failed site could be compensated temporarily by adjacent sites; the impact may be a system-wide capacity degradation.

AVAIL-9 Hardening will be required at jurisdiction-listed high risk areas (eg sites which serve large public gatherings, and critical infrastructure)

PSAs need to know where the system is down to put into effect contingency plans whilst the PSMB service is restored.

AVAIL-10 PSAs will be informed of planned and unplanned outages which impact PSMB services in their jurisdictional area as soon as practicable

PSAs need to know how well the PSMB system is performing.

AVAIL-11 PSAs will have access to on-demand service availability reports describing outage periods which affected their jurisdictions and the respective causes

AVAIL-12 PSAs will have access to monthly service availability reports describing outage periods which affected their jurisdictions and the respective causes

Typical network operators have a business continuity and disaster recovery plan, including risks control and procedures, to prepare for a force majeure event.

AVAIL-13 There will be a business continuity and disaster recovery plan per jurisdiction which will be updated on a yearly basis

2.7 Security

The following requirement reflects the need to physically secure and protect what is considered a critical site. Critical sites include core network facilities as well as radio sites. Physical security may be provided via the use of shelters, fences, surveillance cameras, protected ports, locks, etc.

SECU-1 Sites delivering PSMB services will be protected from unauthorised physical access and equipment tampering

The following requirement highlights the need for proper security credentials in order to access telecommunications facilities. For PSMB services provided by a commercial operator this may include additional vetting, alternatively, adequate training, of existing personnel.

SECU-2 Only PSA-authorised and authenticated personnel will have access to communications facilities supporting PSMB services

The following requirement implies that a process exists to ensure that physical security measures are in place (see ISM 2016).

SECU-3 Access to fixed telecommunications facilities and deployables that provide PSMB services will be accredited by a PSA-designated authority

The following requirement is not meant to imply a physical separation only, but at a minimum logical separation. The use of Virtual Local Area Network (LAN), the use of a separate public land mobile network identifier, and the use of distinct access point name (APN) are such examples.

SECU-4 When using shared resources, public safety traffic should be logically or physically segregated from non-public safety traffic

The following requirement is designed to ensure that messages destined for a particular user or device originate from the right source and have not been tampered with, nor decoded. There may be segments under the control of other entities within the end to end architecture which would require VPN connectivity and service level agreements.

SECU-5 The integrity and confidentiality of PSMB traffic will be ensured as it propagates through the network, including transit over public network segments

The following requirement is designed to reflect the fact that public safety agencies have traditionally relied heavily on mobile VPN service, which is expected to continue.

SECU-6 Mobile Virtual Private Networking will be supported

The following requirement is to ensure that only public safety official/administrator/colleagues with a need-to know have access to the location of public safety users

SECU-7 The geo-location of public safety users will be treated as confidential information and only accessible to PSA-authorised individuals

The following requirement reflects the need to protect media traffic from the end-user device to the network demarcation point, i.e. where connectivity is handed-off to the agency network. For device-to-device communications, with or without a repeater, although the trusted domain is restricted to the device to device links, encryption is required.

SECU-8 The end-to-end security of PSMB services and traffic will apply both when communicating on-network (infrastructure mode) and off-network (device-to-device)

The following requirement is designed to ensure cryptographic keys are protected even if actual master keys used to encrypt/decrypt over-the-air messages, including registration etc., are not transmitted by either the device or the network.

SECU-9 The PSMB capability will ensure that over-the-air exchange of cryptographic keys are confidentiality-protected, integrity-protected and authenticated when delivered over the air

Public safety users have a need for PSMB mission-critical services. Additionally, there are circumstances in which government ministers and other authorized, non-PSA personnel may be granted access to mission-critical services.

SECU-10 Only PSA-authorised and authenticated users will have access to mission-critical PSMB services and features

The following requirement highlights the tendency for most cyber incidents to originate from the internet, i.e. normally outside the agency security domain. For instance, an attack on the PSMB's home subscriber system (a system which authenticates PSMB devices), which stores users (devices) information including all users' master keys, would represent a major cyber incident. .

SECU-11 The network providing PSMB services will have the appropriate levels of protection against cyber incidents

The following requirement reflects the need for PSA agencies to know which PSA visitors are using PSMB resources in their jurisdictions and whether the visitor is authorised to use the PSMB when roaming into their jurisdiction.

SECU-12 PSA-authorised users will have the ability to actively monitor all connected users within their jurisdiction at any time

PSAs need to be made aware of potential cyber-attacks.

SECU-13 PSAs will be informed of suspicious activities, including suspected malicious attempts as soon as is practicable

The following requirement is designed to ensure public safety agencies take proper security measures for applications and devices in their span of control. Discovery of the vulnerability may originate from the device's operating system developer, application developers, the device manufacturer or the network manufacturer(s).

SECU-14 Public safety agencies will be informed as soon as practicable of newly detected security vulnerabilities

The following requirement is to ensure that major security risks are mitigated as early as possible. This may include software patches or new firmware. Other measures may include the blacklisting of a particular application.

SECU-15 Security vulnerabilities will be mitigated as soon as practicable

The following requirement is to ensure that, prior to being allowed to attach to the network, devices are deemed secure and clear of viruses or malicious codes. Bring Your Own Device (BYOD) devices represent potential high-risk end-nodes

SECU-16 PSMB devices will be validated per agency policies before being allowed access to the network and/or services

The following requirement is extracted from the Protective Security Policy Framework (PSPF) mandatory requirements (GOV-12)[30]

SECU-17 For PSMB services contracted from a third-party service provider, third-party service providers will comply with specified requirements of the Protective Security Policy Framework and any other specified protective security protocols.

There is an expectation that to manage subscribers and individual profiles, devices, and applications, PSAs will access the PSMB system through one or more portals. For example, an incident management portal may be used to enable prioritisation and quality of service control. Another portal may be used for trouble-ticketing and other network monitoring functions. The requirement below is to indicate that the interface used by these portals must be secured[31].

SECU-18 The transfer of information between a PSA and the web (business) portal will be secured

2.8 Interoperability

It is important to note that the use of common standards across a system facilitates interoperability. Therefore, the requirements in section 2.11 (Standards) complement those listed in this section.

The following LTE-to-LTE interworking requirement is designed to provide public safety users visiting other jurisdictions (e.g., another state) with the ability to access PSMB services within the visited jurisdiction, pending authorisation from both the home and visited jurisdictions. For example,

[30] If applicable
[31] The Secure File Transfer Protocol (SFTP) is one example

for performance reasons, it may be more advantageous to leverage a visited mission-critical PTT server than the home server. The requirement is contingent on local policies.

INTEROP-1 The PSMB service will support the ability for a public safety user, away from their home jurisdiction, to access (home or visited) PSMB services while in the visited jurisdictions.

The following LTE-to-LTE interworking requirement concerns group affiliation. The requirement is designed to ensure that the visited dispatcher recognises the visitor's identity and profile, and authorises the user to join a specific service group. The requirement is contingent on local policies.

INTEROP-2 The PSMB service will support the ability for a visitor away from their home jurisdiction, to join a group in the visited jurisdiction

The ability for a public safety user to maintain a PSMB session while 'roaming' into a visited jurisdiction is an important tenet of interoperability,

INTEROP-3 Both uplink and downlink seamless mobility will be supported as a public safety user 'roams' from one jurisdiction to another

If jurisdictions deploy different application servers and device clients, interoperability testing should take place to guarantee interoperability

INTEROP-4 Services should be tested across jurisdictions prior to deployment to ensure they don't adversely affect interoperability

In contrast to traditional LMR standards, commercial standards evolve at a much faster pace. This fast pace of evolution represents one of the key challenges for network buildout and sustainability when building a network of networks, e.g. multiple State systems.

INTEROP-5 To maintain service interoperability across jurisdictions, network upgrades (including the introduction of new features) will not compromise interoperability

2.9 Devices

The following requirement is designed to account for all possible device types used by PSA personnel, e.g. devices carried or worn by individuals, installed in vehicles, boats, aircrafts, drones, battery-operated devices for temporary use; relays, sensors and cameras.

DEV-1 PSMB devices will include form factors such as handhelds, vehicular modems, tablets, wearables and machines, and associated accessories

The following requirement is designed to facilitate air-to-ground and maritime operations. These devices are typically designed for the intended operating environment

DEV-2 PSMB devices for airborne and maritime operations will be supported

The following requirement is designed to highlight the fact that some PSMB devices – for example those used by law enforcement or fire response - will require a device-to-device communications capability.

DEV-3 PSMB devices which support device-to-device communications will be made available to PSAs

The following requirement recognises the eventuality of LMR and PSMB services running in parallel.

DEV-4 Public-safety-grade devices should include units which support both existing LMR and LTE services

Public safety officers work in shifts. The following requirement reflects the fact that multiple users may share the same device (across shifts, for example). The profile may include the user identifier, the authorised groups etc.

DEV-5 The PSMB device will allow sharing by multiple users, each with their own profile

The following requirement is designed to indicate that some public safety users may have access to multiple devices, e.g. a vehicular device and a smart phone.

DEV-6 The PSMB service will support the concurrent use of multiple devices by a single user

The following requirement recognises that not all PSA personnel require hardened devices. (E.g., detectives.)

DEV-7 Supported PSMB devices will be comprised of both consumer-grade and public safety-grade devices

The following requirement highlights the public safety-grade nature of devices[32].

DEV-8 Ruggedised/Public safety-grade devices will be suitable for use in the environments and circumstances public safety users operate in. Specifications for these devices will include consideration of appropriate battery life, protection against dust, humidity, shock, heat and vibration.

The following requirement reflects the fact that PSAs often control both ends of the PSMB service: device and application. If the service is provided by a 3rd-party, there is an expectation for a portal to manage devices as well as subscribers and applications.

DEV-9 Public safety agencies will have the ability to remotely provision, configure, disable, and erase the contents of (wipe) supported devices

Fire and emergency medical agencies are often staffed by volunteers. Many of these volunteers use their own devices. The following requirement is contingent on agencies policies but it does not guarantee prioritisation of PSMB services.

DEV-10 Authorised BYODs ("Bring Your Own" Devices) will be provided with access to PSMB services

The following requirement is to ensure devices meet local specifications, including security specifications. This type-approval is different from the radio aspect usually managed by the regulator ACMA.

DEV-11 All PSMB devices will be type-approved by a PSA-designated entity

Because of technology evolution, and unless a device refresh program is in place, the introduction of new network features will not preclude the use of existing devices.

DEV-12 Any new features added to the PSMB capability will be added in a way that ensures all PSMB devices are backward compatible

Given the area size of the country and the remoteness of most of the geography, the radio coverage footprint will be limited geographically. While the provision of PSMB services over the satellite segment remains a desired capability, the limitations of the satellite segment are well understood. Currently known satellite air-interface specifications are different from the PSMB air-interface (i.e.

[32] Ergonomics, MIL-STD 810f/g and IP67 are examples of design criteria

LTE), and there is no guarantee that mission-critical services as specified by 3GPP can be carried over a satellite segment, in view of the limited bandwidth and excessive roundtrip delays.

DEV-13 For remote and any unserved PSMB areas, PSMB devices should include units capable of both terrestrial PSMB access and satellite access

2.10 Integration

It is important to note that while LMR-LTE interworking can be achieved with proprietary techniques, the LTE standards body (3GPP) is in the process of developing specifications for an interworking function. This interworking function applies to both P25 and TETRA Land Mobile Radio technologies. Since legacy LMR services support voice and narrow-band data, the 3GPP scope is limited to so-called mission-critical push-to-talk and mission-critical data. .

The following requirement reflects the basic function, which would enable communications between an end-user using a LMR device and an end-user using a PSMB device.

INTEG-1 A public safety user using the LMR service, and a public safety user using the PSMB service, will be able to communicate with each other

The following requirement presumes that consoles are legacy equipment from the LMR system hence, similar to a non-3GPP access device.

INTEG-2 Dispatchers will be able to monitor and communicate simultaneously with both LMR and PSMB users via a console

The following requirement relates to ongoing work within 3GPP to specify interworking functions to enable LMR to LTE communications.

INTEG-3 LMR to LTE interworking operations will comply with 3GPP standards

The following requirement is needed because P25 and LTE use different speech codecs. As a result, digitised voice from a P25 device may need to be transcoded if it is sent to an LTE device[33]. Transcoding causes degradation to end-to-end voice quality.

INTEG-4 When audio propagates from LTE to LMR, or vice versa, any transcoding will not adversely impair the quality of the communications

[33] It is possible for an LTE device to also support a P25 codec, in which case, transcoding may not be required.

Absent dual-mode capability in all devices, the following requirement is needed while technology migration is ongoing. (Requirement STAND-2 enables that capability.)

INTEG-5 Group communications between PSMB talk-groups and LMR talk-groups will be supported

This requirement is to ensure secure communications between two disparate systems, i.e. with own vocoders, own encryption keys etc[34]. Often PSA agencies operate in a secure mode with some agencies, more than others.

INTEG-6 End-to-end secure communications between a LMR user/console and a LTE user, or between a LMR talk-group and a LTE talk-group, will be supported

2.11 Standards

Standards for mission-critical LTE services are being developed by 3GPP. The first 3GPP specifications which include support of mission-critical communications appear in 3GPP Release 12. The work on mission-critical services (i.e. mission-critical push-to-talk, mission-critical video and mission-critical data) started under Release 13 activities and is continuing under Release 15. 3GPP Release-15 is scheduled to be completed in mid-2018[35]. Separately, testing activities (plugtests) for the validation of equipment against mission-critical push-to-talk conformance have started.

Release 13 is the first LTE release which includes specifications for mission-critical services.

STAND-1 The PSMB service will, as a minimum, use 3GPP Release 13 for baseline specifications

The following requirement refers to the support for mission-critical quality class indicators as defined in 3GPP TS23.203.

STAND-2 The PSMB service will support standard mission-critical quality of service (QoS) parameters

The following requirement refers to the support of priority features as defined in 3GPP TS23.401.

[34] Requirements on encryption in 3GPP TS 22.179 (Rel.14) are currently limited to LTE interworking with LMR standards such as P25 and TETRA only

[35] Note that, traditionally, 3GPP did not embark into the development of applications specifications.

STAND-3 The PSMB service will support standard prioritisation including the ability to pre-empt users and services

The following requirement is to indicate that devices must have passed all required 3GPP testing by an accredited certification body.

STAND-4 PSMB devices will be 3GPP standards compliant

The following requirement is to avoid proprietary clients and application servers, which may hinder interoperability.

STAND-5 Mission-critical applications will comply with existing standards as much as practically feasible

The following requirement is to assist public safety agencies in inter-connecting their back-office network with the PSMB network.

STAND-6 The PSMB network external interfaces will be standards compliant

The requirement is to reflect improvements in the capabilities as standards evolve through introduction of applicable features

STAND-7 The PSMB capability will benefit from latest advances in standards specifications, when applicable.

To evaluate the PSMB service provider, PSAs need to have a good understanding of the process and timeline for supporting relevant public safety features. Vendors generally have one to two major releases per year.

STAND-8 PSAs will be provided with the process and roadmap associated with the implementation of standardised mission-critical feature sets

END OF HLR

3 References

[1] Functional Working Group, “Australia Public Safety Mobile Broadband (PSMB) National Objectives”, September 2017.

[2] 3GPP TS 22.280, “Mission-Critical Services Common Requirements”, June 2017 (www.3gpp.org).

[3] Australian Bureau of Statistics, “ASGS Remoteness Structures”, Edition 2011

[4] UK Home Office. “Public Safety Group Call use metrics”, SA WG2 Meeting #S2-97, May 2013

[5] Mission Critical Communications, “AT&T Exec Highlights Priority, Pre-emption, App Program”, August 28,2017, https://www.rrmediagroup.com/Features/FeaturesDetails/FID/783

[6] ETSI, “First MCPTT Plugtests”, 19-23 June 2017. (http://www.etsi.org/news-events/events/1137-1st-mcptt-plugtest)

[7] National Public Safety Telecommunications Council, “Priority and Quality of Service in the Nationwide Public Safety Broadband Network, Rev 1.4”, August 2015. (http://www.npstc.org/download.jsp?tableId=37&column=217&id=3515&file=PQoS15_003_PQoS_Definition_v1_4_20150817_GB_APPROVED.pdf)

[8] Australian Government, “Information Security Manual - Controls”, 2016.

[9] Australian Government, “Protective Security governance guidelines- Security of outsourced services and functions”, version 1.1, April 2015.

[10] Submissions to the Productivity Commission (from NSW, QLD, VIC, WA, Ambulance Service, Police Federation, ACMA, Optus, Telstra and Motorola), August to November 2015

[11] FirstNet RFP, January 2016: Documents are available https://www.fbo.gov/index?s=opportunity&mode=form&id=706ef840109c2e2a9c7707dc5a8f4009&tab=core&_cview=1

[12] National Public Safety Telecommunications Council & Association of Professional Communications Officials, “Defining Public Safety Grade Systems and Facilities”, May 2014, (http://www.npstc.org/download.jsp?tableId=37&column=217&id=3066&file=Public_Safety_Grade_Report_140522.pdf)

[13] Australian Government, Dept. of Communications, “Mobile Blackspot Programme – Guidelines”, version 1.1, December 2014

[14] “Answering the Call: Communications Lessons Learned from the Pentagon Attack,” US Public Safety Wireless Network Program, January 2002.

[15] Yannick Lair and Georg Mayer, “Mission Critical Services in 3GPP,” June 20, 2017. (http://www.3gpp.org/news-events/3gpp-news/1875-mc_services)

[16] National Public Safety Telecommunications Council Broadband Working Group, “Mission Critical Voice Communications Requirements for Public Safety,” (http://www.npstc.org/download.jsp?tableId=37&column=217&id=2055&file=Mission%20Critical%20Voice%20Fu)

[17] “ETSI and TCCA hold first interoperability trials for LTE mission critical communication,” June 12, 2017. (http://www.etsi.org/news-events/news/1198-2017-06-news-etsi-and-tcca-hold-first-interoperability-trials-for-lte-mission-critical-communication)
[18] 3GPP TS 22.179: "Mission Critical Push To Talk (MCPTT) over LTE; Stage 1".
[19] ITU-R M.2377-0, “Radio communications and Objectives for Public Protection and Disaster Relief (PPDR)”, July 2015
[20] Department of Homeland Security, “Public Safety Statement of Requirements for Communications and interoperability”, Volume II, Version 1.2, August 2008
[21] Department of Homeland Security, “Assessing Video Quality for Public Safety Applications Using Visual Acuity”, DHS-TR-PSC-12-11, November 2012
[22] U.S. Federal Communications Commission Public Safety and Homeland Security Bureau, “In the Matter of Requests for Waiver of Various Petitioners to Allow the Establishment of 700 MHz Interoperable Public Safety Wireless Broadband Networks,” Order DA 10-2342, Public Safety Docket No. 06-229, December 10, 2010
[23] TIA TSB-88.3-C, “Wireless Communications Systems Performance in Noise and Interference Limited Situations – Part 3: Performance Verification”, February 2008
[24] TIA 222 – Rev G-2, “Structural Standards for Antenna Supporting Structures and Antennas”, 2009
[25] National Public Safety Telecommunications Council and the Defence Research and Development Canada’s Centre for Security Science, “Broadband Deployable Systems in the Nationwide Public Safety Broadband Network,” April 2017. (http://npstc.org/download.jsp?tableId=37&column=217&id=3903&file=NPSTC_CSS_BB_Deployable_Systems_Report_Final_170403.pdf)
[26] Agreement between Los Angeles Regional Interoperable Communications System Authority and Motorola Solutions Inc., for LARICS- Public Safety Broadband Network, Agreement no. LA-RICS 008, 2014
[27] Verizon Wireless National Government Operations, “FSSI Wireless (BPA QTA-0-12-PS-B-0006)”, prepared for the General Services Administration, Volume III, Revised April 2013

4 APPENDIX

4.1 Performance Requirements

This section provides a set of performance recommendations which illustrate how a commercial grade service is distinguished from the public safety grade service required by the PSMB capability. The list provided below is illustrative, but not exhaustive. When the PSMB capability is implemented, service level agreement(s) between PSAs and the public safety service provider will feature a more complete set of key performance indicators.

The PSMB will be designed to support target uplink/downlink data rates over a large fraction of a PSMB service area, as determined by individual jurisdictions. Different uplink/downlink data rate targets may be specified in different areas, owing to the operational requirements of public safety officials, and device types used by first responders. These data rates are expected to be achievable at the periphery of a cell's coverage area, with higher average speeds achievable across the cell area.

The most bandwidth-intensive service used by PSAs is video. Hence, it is reasonable to assume that quality video must be supported across most of the PSMB service area. Video can be encoded using a variety of bit rates and encoding algorithms. Studies on video quality (e.g.[21]) indicate a large range of acceptable data rates between 64 kbps and 2 Mbps, depending on operational requirements.

With the growing interest for more usage of (tactical) video by public safety, there is also an expectation that its usage, more particularly live uplink video, may become a constraining design factor[36]. Testing was performed to provide recommendations on data rates for tactical video based on the complexity of the target. Recommendations suggested 256 kbps and 512 kbps as acceptable video data rates[21].

Therefore, the following performance requirement defines the desired minimum data rates achieved over a PSMB coverage area by portable PSMB devices. The data rates selected are based on minimum data rates specified by the US Federal Communications Commission in [22]. These data speeds are expected to provide reasonable quality of service for most public safety applications.

PR-1 The PSMB portable service bandwidth should be characterised by a minimum uplink (device to network) user throughput of 256 kbps and minimum downlink (network to device) throughput of 768 kbps[37]

---

[36] Although high data rates may be achievable in an urban area in view of the typically denser network, it is not likely to be the case in other areas.

[37] Performance in a cell is subject to interference from users camped in other cells. This interference is often reflected by a loading factor, leading to the specification of an interference margin. On a dedicated spectrum, owing to the relatively small number of public safety users, the loading can be less than 35%, but on a non-

Since vehicle-mounted PSMB devices can have a more effective antenna system than hand-held portable devices, vehicle-mounted devices can achieve a higher throughput at the same distance. (An example of this is the situation where a portable device and an emergency vehicle are co-located. In this scenario, the vehicle-mounted device will experience higher throughput than the hand-held portable device.). At these rates, a public safety user will experience a better resolution video link than with a portable. The following performance requirement defines the minimum data rates achieved over a PSMB coverage area when users are on highways and other principal roads.

PR-2 The PSMB vehicular service bandwidth on major and secondary roads should achieve a minimum uplink user throughput of 1 Mbps and minimum downlink throughput of 1 Mbps

The following performance requirement is designed to ensure as much coverage as possible in remote areas, where distances between network antenna towers are typically large[38].

PR-3 The PSMB vehicular service bandwidth in remote areas, except for major and secondary roads (as covered in COV-8), should achieve a minimum user throughput of 64 kbps on the uplink and 256 kbps on the downlink

The following performance requirement defines the desired range of coastal PSMB services. The range should extend to the water limits of state jurisdiction.

PR-4 The PSMB maritime service bandwidth should achieve a minimum user throughput of 1 Mbps on the uplink and 1 Mbps on the downlink

The design of a wireless network, and the number of sites, is influenced by the desired coverage reliability level, hence a design margin[39]. The higher the margin, the larger the number of sites required. A coverage reliability figure of 95% means that, when accounting for that design margin, the targeted data rates are achieved over 95% of the coverage footprint. Networks designed for higher coverage reliability levels achieve a more homogenous service across the service area. LMR network designs generally aim at coverage reliability figures above 95% (e.g. 97%) in metropolitan areas and lower coverage reliability figures in remote areas. A reliability figure of 95% or less is

---

dedicated spectrum, when sharing spectrum with consumers, it is typical to assign a 70% value. For reference, FirstNet suggested a 50% loading

[38] 3GPP standards specify a high-power class specifically to enhance radio range for public safety systems. While the standard addresses a limited number of bands, it does not preclude the extension of the specification to other spectrum bands. For feasibility, the identification of a spectrum band will require an interference study.

[39] These figures are for area coverage reliability figures. Similar figures can be derived for cell edge reliability.

typical in a commercial network metropolitan design. Coverage reliability is often verified in an LMR network deployment using extensive drive tests.[40]

The following performance requirements specify PSMB (coverage) reliability requirements in varied coverage areas[41].

PR-5 The PSMB service should provide portable indoor coverage within PSA-designated facilities with at least 95% reliability

PR-6 The PSMB service should provide portable outdoor coverage in major cities and regional towns with at least 97% reliability

PR-7 The PSMB service should provide portable outdoor coverage in and around jurisdiction-listed major risk areas with at least 97% reliability

PR-8 The PSMB service should provide mobile coverage along roads and railroads with at least 95% reliability

PR-9 The PSMB service should provide mobile coverage in rivers, lakes and coastal areas with at least 95% reliability

PR-10 For areas not covered by PR-5 to PR-9, the PSMB service should provide mobile coverage with at least 95% reliability

The following performance requirement is designed to ensure that the number of normal session terminations exceeds the number of (involuntarily) dropped sessions. Less than 1% failure should be the norm.

PR-11 The retainability rate of PSMB services should be at least 99%

The following performance requirement is designed to ensure that the number of successful access attempts exceeds the number of failed attempts. Failed attempts may include network attach failures, connections failures, failure to setup bearers, etc. A failure rate of less than 1% should be the norm.

PR-12 The accessibility rate of PSMB services should be at least 99%

The following performance requirement is designed to ensure that the number of successful handovers exceeds the number of failed handover attempts. A failure rate of less than 1% should be the norm[42].

[40] See, e.g., TIA TSB-88 series of guidelines originally intended for P25 deployments
[41] Figures may vary on a State basis based on experience with impairments due to terrain, and associated costs.

PR-13 The success rate of handover of sessions should be at least 99%

The resolution of radio coverage maps will account for propagation modelling limitations and the resolution of the clutter/terrain database. Because of the size of the cells, it is typical to use high resolution in urban and suburban environments (e.g. 10mx10m or less) and a lower resolution in rural environments (30mx30m)[43].

PR-14 Radio coverage maps will have a resolution of 30m by 30m, or better

The availability of PSMB services is contingent on the uptime of the PSMB network. Excluding natural hazards, and acts of sabotage or vandalism, the failure rate of communications equipment, the amount of redundancy in the network nodes, and in the architecture, are the usual determining factors in estimating the average system availability. Tower structure reinforcement, power backup, and use of shelters represent hardening measures to supplement equipment availability, but not improve it. From an equipment perspective only, an average system availability of 99.99% is achievable, given that the bulk of downtime outages is due essentially to radio nodes[44]. The performance requirement should be seen as an objective.

PR-15 The service availability, on a jurisdiction basis, should be at least 99.99% as a monthly average[45]

---

[42] This is for intra-RAT (i.e. LTE-to-LTE) and intra-frequency (i.e. no frequency change)

[43] Urban, suburban and rural, which are terms usually used to (grossly) categorize a radio propagation environment classification, are not directly related the ABS Remoteness classification.

[44] It is usual to design a wireless network with the transport segment and the core specified at greater than 99.999%, assuming a mean-time-to-repair of 4 hours. This is usually achieved through path diversity, geo-redundancy and duplex equipment configurations. The radio access network is often the weakest link since it is not economically feasible to deploy redundant radio sites; for radio site whose equipment uses 1:n redundancy at the module level, or techniques such as RF cross-connect, the availability figure could be slightly improved.

[45] To quote a few figures:

- The 2014 agreement between Los Angeles County and their LTE vendor states: "…the hardware and software Components of the PSBN will remain fully operational and available at a rate of 99.99% measured on a monthly basis."
- Per Victoria Government's submission to the Productivity Commission, "Victoria's Mobile Data Network (MD) core network service availability has performed well in excess of 99.99% over the last nine years"
- FirstNet's Statement of Objectives calls for a "99.99% user service availability as measured in a rolling 12-month window within each reporting area"
- Per the UK Home Office National Audit Office, "The (Airwave) network has averaged 99.9% availability since April 2010"
- Verizon Wireless contract for federal government services states "Cell availability of 99.90% as a monthly average…measured across the entire network"

The following performance requirement is designed to ensure rapid service restoration after an outage with major impact on the PSMB service. Depending on the severity, it implies availability of close-by technicians and the availability of spares. The following performance requirement relates to an outage of critical severity which may include the loss of a radio site, of the core network, of a single sector, of a backhaul link, etc. There may be definition of additional (less critical) severity levels which would not warrant such quick restoration times[46].

PR-16 The average time to restore the PSMB service should be no more than 4 hours in metropolitan areas, 6 hours in regional areas, and 8 hours in remote areas[47]

This performance requirement pertains to the historical logging of outages events. Such data is needed to support the continuous improvement of the PSMB capability.

PR-17 Historical PSMB service availability data describing outage periods and the respective causes should be stored for a period of at least 10 years

[46] Although there is an expectation that the PSMB network operator will be managing network operations, notifications of an outage may originate from a PSA administrator

[47] Time is from notification/detection of the outage to complete resolution

4.2 Coverage Factors

4.2.1 Service Area

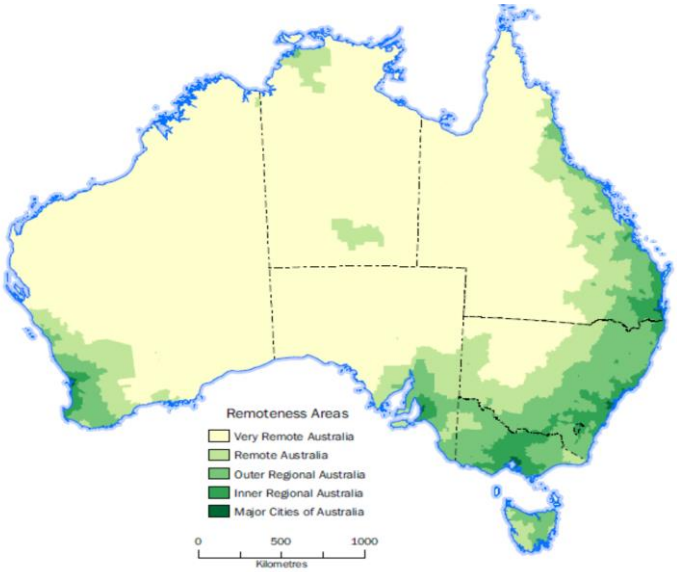
Incidents requiring public safety agency response can happen anywhere. With their knowledge of the region, more particularly zones that are more prone to incidents or other critical areas, jurisdictions know best what fraction of their respective region should require permanent coverage. As a result, PSAs must be able to specify where PSMB coverage is required to support day-to-day, incident, and planned event operations. Required coverage areas include, for example, transportation networks (e.g., roads, bridges, tunnels, passenger and freight rail lines, rivers), critical infrastructure (e.g., hospitals, electric power facilities, public safety facilities), sports stadiums, concert venues and locations with (historical) high incidences of crime/accidents. PSAs must be able to specify the coverage that is required to meet their specific operational needs.

On the other hand, public safety agencies expect PSMB coverage from deep inside buildings to unpopulated remote areas, to coastal zones. The extent of geographical coverage is much wider than is typical with commercial wireless service.

Australia contains large, uninhabited areas. PSAs can also be called upon to respond in remote areas not served by the PSMB fixed infrastructure. The reliance on (rapid) deployables and/or satellite service will be key to provide temporary coverage in those areas. Depending on the functionality provided by deployable assets, satellite services may be used to link the deployable infrastructure to public safety agencies' networks.

Regional Classification

The Australian Bureau of Statistics, when defining Remoteness structures, defined five (5) regions as shown below



4.2.2 Coverage Reliability

The design of a wireless network, and the number of sites, is influenced by the desired coverage reliability level, hence a design margin, also referred to as the shadowing margin. The margin accounts for variability in the RF environment due to obstructions, terrain effects and other factors. Higher margins result in a more robust service, and a larger number of base station sites. A coverage reliability figure of 95% means that, when accounting for that design margin, the targeted data rates are achieved over 95% of the coverage footprint. Networks designed for higher coverage reliability levels achieve a more homogenous service across the coverage area. LMR network designs generally aim at coverage reliability figures above 95% (e.g. 97%) in metropolitan areas and lower coverage reliability figures in remote areas. A reliability figure of 95% or less is typical in a commercial network metropolitan design. Coverage reliability is often verified in an LMR network deployment using extensive drive tests.

4.2.3 Desired Service Rates

PSAs must be able to specify the grade of service required over different regions. Grades of service specify, for example, the minimum uplink/downlink data rates the area has been designed to support. Coverage of an LMR system is defined as a (RF) footprint whose contour represents the edge of a service area in which voice service is supported. The region across which voice is delivered within specified audio quality requirements defines the LMR site coverage area. Given that the PSMB service allows for the provision of multiple applications, including voice, a decision must be made on what types of service should be guaranteed within that footprint or, equivalently, at its edge (so-called cell edge). Since applications require different data rates (or throughput), the desired service will determine the range of a cell, and, hence the number of sites which must be deployed. The achievable range is typically limited by the device-to-base station-site communications link (uplink).

For example, a broadband network designed to support a 256 kbps uplink user throughput at cell edge will result in a smaller required number of sites than a network designed to support 1 Mbps at cell edge. During the early debates in the U.S. on broadband public safety networks, the U.S. spectrum regulator, the Federal Communications Commission (FCC), defined the design criteria as “256 kbps uplink and 768 kbps downlink”. The selected uplink rate was dictated by the need to support reasonable quality (compressed) video feed from a user’s device. It is worth emphasizing that for a given cell edge supporting a 256 kbps user throughput, applications requiring a lower throughput, such as text messaging, geo-location and voice, will be supported beyond the designed range. Higher data rates will be achieved as the device moves towards a cell site.

If there is a desire to require a PSMB coverage comparable to LMR coverage, especially when planning for the LMR migration to PSMB, proper consideration would need to be given to the link budget, device transmit capabilities, use of receive diversity at cell sites, and other factors.

4.3 Mission-Critical voice

4.3.1 Definition

In preparation for the United States' planned construction of a nationwide public safety LTE network, the US's National Public Safety Telecommunications Council Broadband Working Group drafted a requirements document to "provide a basis for a common understanding of the meaning of and the multiple requirements of mission critical voice." Key functionality required by a Mission Critical Voice service include (bulleted text below extracted directly from [16]):

[*begin excerpted text*]

- **Direct [Mode] or Talk Around:** This mode of communications provides public safety with the ability to communicate unit-to-unit when out of range of a wireless network OR when working in a confined area where direct unit-to-unit communications is required.
- **Push- to- Talk (PTT):** This is the standard form of public safety voice communications today - the speaker pushes a button on the radio and transmits the voice message to other units. When they are done speaking they release the Push-to-Talk switch and return to the listen mode of operation.
- **Full Duplex Voice Systems:** This form of voice communications mimics that in use today on cellular or commercial wireless networks where the networks are interconnected to the Public Switched Telephone Network (PSTN).
- **Group Call:** This method of voice communications provides communications from one- to-many members of a group and is of vital importance to the public safety community.
- **Talker Identification:** This provides the ability for a user to identify who is speaking at any given time and could be equated to caller ID available on most commercial cellular systems today.
- **Emergency Alerting:** This indicates that a user has encountered a life- threatening condition and requires access to the system immediately and is, therefore, given the highest level or priority.
- **Audio Quality:** This is a vital ingredient for mission critical voice. The listener MUST be able to understand without repetition, and can identify the speaker, can detect stress in a speaker's voice, and be able to hear background sounds as well without interfering with the prime voice communications.

[*end excerpted text*]

Except for Full Duplex voice, the above attributes constitute what is commonly regarded as mission-critical voice characteristics.

4.3.2 Mission-critical PTT

The term ‘Mission-Critical Push-to-Talk (MCPTT)” is commonly used to describe the wireless voice service required to support public safety operations. MC PTT services differ from the voice services offered by today’s commercial wireless networks in a number of important ways:

- In contrast to today’s commercial voice communications, most public safety voice communications is team-based: for example, a dispatcher talking to a large team (100s of first responders) in the field, or public safety teams communicating amongst themselves to coordinate incident response. Incident response may result in large numbers of public safety users present within the coverage area of a cell. 900 radio users were on scene at the U.S. Pentagon after the terrorist attacks on September 11, 2001, for example [14]. Today’s commercial wireless networks do not provide the scale needed to provide such service unless group communications features are supported both on the network and on the devices.
- Public safety voice services have stringent requirements on security, reliability, availability, performance and scalability. These requirements are typically far and above the requirements supported by today’s commercial wireless networks.

To meet these unique requirements, public safety agencies to date have relied on purpose-built, Land Mobile Radio (LMR) technologies. Examples of these technologies include Project 25 – a technology used in Australia, Canada, and the United States – and TETRA – a technology used predominantly in Europe and other parts of the world.

LTE has been selected as the technology of choice for next-generation public safety wireless networks in the United States (FirstNet), the UK (Emergency Services Network), Korea (SafeNet) and other countries. As a result, LTE standards enhancements are being developed in the LTE standards body (3GPP) to support mission critical voice services comparable to the services provided by Project 25 and TETRA (see [18]). Early proof of concept trials of LTE’s MCPTT service have already been conducted, including an ETSI and TCCA interoperability ‘plugfest’ held in June 2017 [17].

MCPTT is characterized by very low latencies. Public safety officials use the following law enforcement communication scenario to demonstrate the need for quick call set-up times and low audio propagation delays: “…fire at will.” Call ends. New call: “Don’t shoot! Don’t shoot!”

3GPP specifications specify a number of performance requirements that characterize MCPTT [18]. For example:

- “Mouth-to-ear latency … that is less than 300 ms for 95% of all voice bursts.”

- "MCPTT Access time [of] less than 300 ms for 95% of all MCPTT Request[s]"[48].

[48] 'Access time' measures the delay from the instant a PTT request is sent from a device and 'permission to speak' is granted by the network.

4.4 Video Quality

Scenario	General Elements	Classification	Characteristics (75-percent perfect)	Positive ID (90-percent accuracy)
Bright light, low motion, large target	64 kbps, CIF	64 kbps, CIF	64 kbps, CIF	128 kbps, CIF
Bright light, low motion, small target	128 kbps, VGA	128 kbps, VGA	128 kbps, VGA	128 kbps, VGA
Bright light, high motion, large target	64 kbps, CIF	64 kbps, CIF	128 kbps, CIF	*1024 kbps, CIF
Bright light, high motion, small target	128 kbps, VGA	128 kbps, VGA	128 kbps, VGA	256 kbps, VGA
Dim light, low motion, large target	128 kbps, CIF	128 kbps, CIF	256 kbps, CIF	512 kbps, CIF
Dim light, low motion, small target	256 kbps, VGA	256 kbps, VGA	512 kbps, VGA	512 kbps, VGA
Dim light, high motion, large target	128 kbps, CIF	256 kbps, CIF	512 kbps, CIF	*1024 kbps, CIF
Dim light, high motion, small target	512 kbps, VGA	512 kbps, VGA	1024 kbps, VGA	*2048 kbps, VGA
Variable light, low motion, large target	256 kbps, CIF	512 kbps, CIF	512 kbps, CIF	*1024 kbps, CIF
Variable light, low motion, small target	256 kbps, VGA	1024 kbps, VGA	1024 kbps, VGA	*2048 kbps, VGA
Variable light, high motion, large target	256 kbps, CIF	1025 kbps, CIF	*1024 kbps, CIF	*1024 kbps, CIF
Variable light, high motion, small target	512 kbps, VGA	512 kbps, VGA	*2048 kbps, VGA	*2048 kbps, VGA

Note: CIF→ 352 x 288 pixels and VGA → 640x480 pixels.

The above Table of recommendations reflects a summary of testing using visual acuity as a basis for video quality assessment under a variety of scenarios. All original video clips were encoded using H.264 at a frame rate of 29.7 frames per second (fps) using multiple bit rates. More information can be found in [20].

5 List of Acronyms

3GPP	3rd Generation Partnership Project
ABS	Australian Bureau of Statistics
AC	Access Class
API	Application Programming Interface
APN	Access Point Name
BYOD	Bring Your Own Device
CIF	Common Intermediate Format
COAG	Council of Australian Governments
DAS	Distributed Antenna System
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
fps	Frames Per Second
FWG	Functional Working Group
HLR	High-Level Requirements
ID	Identifier
ITU	International Telecommunications Union
kbps	kilobits per second
LAN	Local Area Network
LMR	Land Mobile Radio
LTE	Long Term Evolution
m	Metre
M2M	Machine-to-Machine
Mbps	Megabits per second
MCPTT	Mission-Critical Push-to-Talk

P25	Project 25
PSA	Public Safety Agency
PSMB	Public Safety Mobile Broadband
PSPF	Protective Security Policy Framework
PSTN	Public Switched Telephone Network
PTT	Push-to-talk
QoS	Quality of Service
RF	Radio Frequency
SOC	Senior Officials Committee
SWAT	Special Weapons and Tactics
TCCA	TETRA and Critical Communications Association
TETRA	TErrestrial Trunked RAdio
USIM	Universal Subscriber Identity Module
VGA	Video Graphics Array
VPN	Virtual Private Network

1185