



**NSW Telco Authority RFT 10013061
RFI NSWTA 104S FILE 17/71608**

National Public Safety Mobile Broadband Capability Request For Information

Response from University of Melbourne Centre for Disaster Management and Public Safety

Lead Author: Geoff Spring Senior Industry Advisor

**Co - Authors: David Williams Senior Industry Advisor
Ged Griffin Senior Industry Advisor**

10 January 2018

Section	Table of Contents	Page No
1.0	Introduction	3
2.0	Purpose	3
3.0	Definition of Critical Infrastructure	4
4.0	Australia's Mission Critical Public Safety Communications Ecosystem	4
5.0	The Public Safety Communications Sector	5
6.0	Response Structure	6
7.0	Executive Summary	6
8.0	PSMB Funding and Resourcing	8
9.0	Advice to the Council of Australian Governments	9
10.0	Use Cases in determining a PSMB Capability	13
11.0	Spectrum	14
12.0	Public Safety Apps	15
13.0	PSMB Business Case	15
14.0	Transparency	16
15.0	Consultation	16
16.0	Public Safety Communications Roadmaps	16
17.0	Federated Capability	18
18.0	International Performance Measurement and Monitoring	18
19.0	Sharing Information and Research Outcomes	19
20.0	Standards	20
21.0	Time Frame	21
22.0	Analysis of Q&A at the PSMB Industry Briefing	21
23.0	Conclusion	22
	Acronyms and Web Addresses	23



Response to the Request For Information regarding the National Public Safety Mobile Broadband Capability issued by the NSW Telco Authority on behalf of Australian Governments and Territories

1.0 Introduction

The University of Melbourne's Centre for Disaster Management and Public Safety (CDMPS)¹ welcomes the opportunity to respond to the Request for Information (RFI) relating to a national Public Safety Mobile Broadband (PSMB) capability issued by the New South Wales Telco Authority on behalf of Australian Governments and Territories.

This response is made by the CDMPS as an "individual party" with a strong interest over a period of time in the provision of a PSMB capability for Australia's Public Safety Agencies (PSAs) and First Responders.

This response is consistent with the CDMP's strategic intent to support multi-disciplinary collaboration between researchers, government, industry, PSAs and the community in delivering exceptional public safety outcomes in terms of increased community safety resilience, enhanced decision making capabilities and public safety outcomes.

This response continues to build upon and references previous CDMPS responses to a range of Australian Government and Federal Government Department Discussion Papers related to individual components of the mission critical public safety communications ecosystem.

2.0 Purpose

The purpose of this response is to continue to identify in the context of the PSMB RFI:

- (a) The need for the Australian Government to recognise Australia's mission critical public safety communications ecosystem as Critical Infrastructure and that a PSMB capability is an essential component of this ecosystem;
- (b) The PSMB RFI is one of a series of Australian Government and Federal Government Department publications *independently* addressing matters that will influence and impact public policy, strategy, and regulatory settings associated with the evolution of the ecosystem and hence the public safety of all Australians;
- (c) The need to continue to raise the profile, understanding and awareness of the mission critical public safety communications ecosystem in the public safety market and with political and bureaucratic decision makers, PSAs and First Responders, and all Australians.

¹ <http://research.unimelb.edu.au/cdmips>

3.0 Definition of Critical Infrastructure

In previous CDMPS responses to Australian Government and Federal Department Discussion Papers the following definition of *critical infrastructure* by the Trusted Information Sharing Network (TISN)² within the Federal Attorney General's Department has been used:

"Those physical facilities, supply chains, information technologies and communication networks, which if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security".

In this response to the PSBM RFI the enhanced statement about critical infrastructure produced by the Critical Infrastructure Centre³ and shown in Figure No 1 has been adopted. The enhanced statement illustrates the growing complexity of the policy, strategy and operational environment in which decisions related to a PSMB capability must be made:

*"Critical infrastructure underpins the functioning of Australia's society and economy and is integral to the prosperity of the nation. Commonwealth and state and territory governments share the following definition of critical infrastructure: **'those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation or affect Australia's ability to conduct national defence and ensure national security'**. Secure and resilient infrastructure ensures we have continuous access to services that are essential for everyday life, such as food, water, health, energy, communications, transport and banking. It also supports productivity and helps to drive the business activity that underpins economic growth".*

Critical Infrastructure Statement produced by Australia's Critical Infrastructure Centre

Figure No 1

4.0 Australia's Mission Critical Public Safety Communications Ecosystem

This response to the PSBM RFI considers the mission critical public safety communications ecosystem illustrated in Figure No 2 to be a closed complex system *currently* comprising following components:

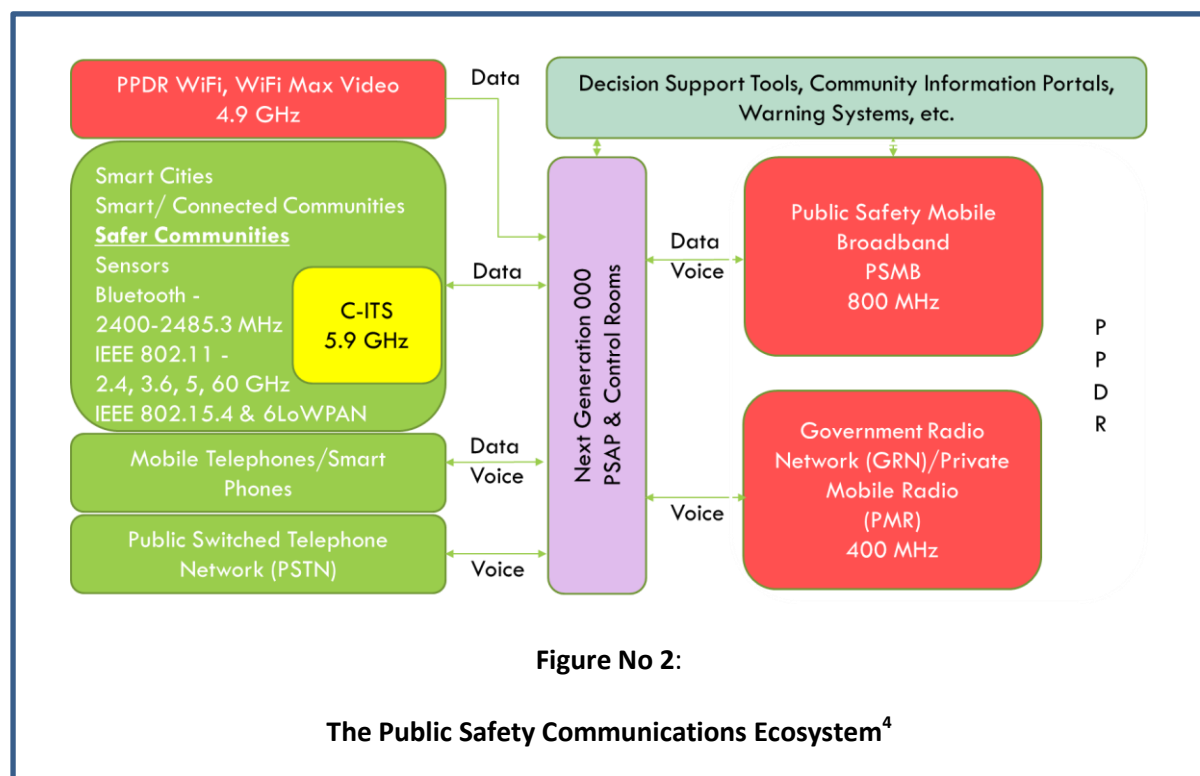
- Public communication devices and services
- The Triple Zero Service
- PSA Communication Centres
- PSA Land Mobile Radio Networks
- The interfaces between these components
- PSA human resources

² https://www.tisn.gov.au/Pages/Cyber_security.aspx

³ <https://www.ag.gov.au/Consultations/Documents/critical-infrastructure-bill/CIC-factsheet-what-is-the-critical-infrastructure-centre.pdf>

In a manner similar to the growing complexity of the policy, strategy and operational environment of critical infrastructure the mission critical public safety communications ecosystem is progressively moving from an analogue or digital *voice* environment, to a *digital data* and *IP based environment* within the mainstream of information communications and technologies.

The PSMB capability will be a new and *transformative* component of the ecosystem built upon the expectation of PSA innovation in service delivery resulting in enhanced decision making capabilities contributing to improved community safety resilience and public safety outcomes.



5.0 The Public Safety Communications Sector

For the purpose of this RFI response and for broader research the mission critical public safety ecosystem will be considered as being a Sector or “vertical” of the Public Safety Market.

The Australian Government and its Federal Departments and Agencies over recent years have issued a series of independent Discussion Papers relevant to the ecosystem for public comment.

Analysis of these responses shows that 145 organisations contributed 203 responses of which Industry Associations were the top contributors with 37 responses (25.5%) followed by specific industry organisations with 35 responses (24.1%) and Government Departments and Agencies with 30 responses (20.7%). Significantly PSAs only contributed seven responses or 4.8% of the total responses representing a lost opportunity to make their positions known in relation to the matters being canvassed in these Discussion Papers including the PSMB capability.

The successful delivery and utilisation of a national PSMB capability will depend on an active program of consultation and engagement with PSAs and First Responders. The low level of

⁴ Ged Griffin Industry Advisor CDMPS University of Melbourne

engagement by PSAs with the Federal Government and its Departments needs to be investigated, identified and addressed in the spirit of collaboration expressed in the Ministerial Statement for the PSMB Early Market Engagement.

In contrast Industry Associations make a significant contribution to influencing government policy development through the public consultation process used by the Federal Government and its Departments.

6.0 Response Structure

The structure adopted for this PSBM RFI response is a gap analysis between the PSMB RFI and the international body of knowledge regarding PSMB capability. This body of knowledge has over past years developed significantly and is continuing to do so as the United States, the United Kingdom, South Korea, Europe and Canada progress their projects to provide their PSAs and First Responders with a PSMB capability in the context of the global Public Protection and Disaster Recovery (PPDR) continuum.

The content of this response also draws on information in the public domain regarding the current status of these international PSMB projects and from the public safety communications stream of the CommsConnect Conference⁵ held in Melbourne in November 2017.

Senior executives from these international PSMB projects attended the CommsConnect Conference to share information and lessons learned with Conference Delegates through individual presentations and Panel Sessions regarding PSMB.

The PSMB senior executives were joined by the CEO of the TCCA⁶ at an Industry Masterclass organised through its local Australian chapter, the ATCCF⁷. The TCCA coordinates global efforts towards the development of mission critical Broadband standards working with the 3GPP and ETSI standardisation organisations and government agencies.

These executives also participated in a closed session (*excluding industry representatives*) facilitated by the Australian Radio Communications Industry Association (ARCIA)⁸ to provide the opportunity to meet with Australian government bureaucrats and PSA representatives. The Federal Government bureaucracy also chose the CommsConnect Conference to release information about the impending PSMB RFI.

There has probably never been a better opportunity for Australia to leverage the global body of knowledge regarding PSMB capability and its impact on the mission critical public safety communications ecosystem more generally.

7.0 Executive Summary

The principle underpinning the gap analysis provided in this PSMB RFI response is that at this point in time the PSMB capability is about the carriage of “data” (text, images, video, spatial, temporal) and not “voice”.

⁵ <http://www.comms-connect.com.au/>

⁶ <https://tcca.info/>

⁷ <http://www.criticalcommsforum.com.au/>

⁸ <http://www.arcia.org.au/>

This data will be used with public safety specific applications and devices utilising machine to machine learning and artificial intelligence to provide enhanced decision making capabilities by PSAs, First Responders and all Australians to deliver increased enhanced community resilience and public safety outcomes.

The outcomes from the gap analysis contained in this response are summarised below in terms of Risks and Opportunities with further explanation to support these outcomes provided in the body of this response.

Risks

- a. There is no evidence of a PSMB Business Case or Use Cases to support a Business Case.
- b. There is no evidence of a national strategy to inform the public safety community about the PSMB capability.
- c. There is no evidence of dedicated funding and resources to support the process of securing a PSMB capability.
- d. The outcomes from the PSMB RFI evaluation will not necessarily identify for the Council Of Australian Governments (COAG) the changes in the policy, strategy and operational environment required for the PSMB capability and the mission critical public safety communications ecosystem more generally and the relationship to other significant related Australian Government policies.
- e. The inadequacy of the PSMB RFI time frame to provide for meaningful stakeholder engagement will potentially impact the quality of the outcomes from the process and the advice to COAG.
- f. In recognition that Long Term Evolution (LTE) technology is neither a competitive or substitutional alternative to Land Mobile Radio (LMR) both capital and operational investment in networks will need to continue for the foreseeable future.
- g. As a result of spectrum auctions and a move in PSMB service delivery models away from the need for dedicated public safety spectrum the value of the 800 MHz spectrum current reserved for public safety use may have been diminished.

Opportunities

- a. The opportunity for the Australia Government to consider the recommendation of the House of Representatives Standing Committee on Infrastructure, Transportation and Cities in 2016 that *mission critical public safety communications be considered as critical infrastructure*.
- b. The opportunity to provide a secure safe working environment for Australia's First Responders as they attempt to keep all Australians safe from harm by effectively and efficiently sharing intelligence generated through use of the PSMB capability and the mission critical public safety communications ecosystem more generally.
- c. The opportunity to leverage the recognition of mission critical public safety communications as *critical infrastructure* to formally involve Infrastructure Australia and the Infrastructure and Project Financing Agency to manage the introduction of private sector involvement and

investment in the public safety market and the evolution of the mission critical public safety communications ecosystem.

- d. The opportunity to formally constitute a national co-ordination body to provide collaborative leadership, strategic oversight and policy direction to the evolution of the mission critical public safety communications ecosystem.
- e. The opportunity to provide increased transparency and clarity about the governance, strategic direction and underlying processes to support the evolution of the mission critical public safety communications ecosystem.
- f. The opportunity to establish a trusted relationship between the public safety community, governments, industry and academia to address the impact of public expectations, and technological change in conjunction with the opportunity for organisational and cultural change that a PSMB capability will present.
- g. The opportunity to establish a research capability leveraging international experience to support Australia's PSAs and First Responders in using the PSMB capability to facilitate innovation in enhanced decision making, personal protection, productivity, and public safety outcomes.
- h. The opportunity for the public safety community to develop specific public safety "Apps" for use in conjunction with the PSMB capability.

8.0 PSMB Governance Funding and Resourcing

This response acknowledges the collaboration between the Federal Government and the States and Territories to establish interim governance arrangements consisting of a Senior Officers Committee (SOC) and a Functional Working Group (FWG) to produce the RFI for the PSMB capability.

However it is understood that there have been no dedicated resources or funding allocated to the development of the RFI and that the SOC and FWG members have been required to continue to perform the duties of their appointed positions.

This approach is consistent with that taken over past years by different governments where there has been reluctance to fund and resource a dedicated project team to provide a PSMB capability for Australia's PSAs and First Responders.

This reluctance has been broadly based around the perceived inability of PSAs to articulate the need for a PSMB capability particularly in relation to the need to provide dedicated spectrum to support this capability.

The RFI appears to continue this approach as it asks industry to absorb the cost of providing advice about its capacity to provide and deliver a PSMB capability within a set of Objectives and High Level Requirements together with the option of funding a possible Proof of Concept trial so that advice on the evaluation of the RFI responses can be provided to COAG in February 2018.

The PSMB RFI advises that the outcome of the RFI process or market engagement is to inform Australian governments' decision making around future federated PSMB implementation and that RFI responses are to limit any cost information to that associated with the Proof of Concept trial.

Given that evidenced based costing has previously been a major hurdle preventing the PSMB capability moving forward it should be expected that COAG will be seeking advice on the cost impact and expected benefits of possible service delivery models in a federated PSMB implementation.

This approach contrasts with the approach taken by international PSMB Projects where Governments have provided considerable funding and resources to establish dedicated governance and organisational arrangements to provide leadership and co-ordination of the broad range of activities required to progress planning and decision making for their respective PSMB projects through engagement with PSAs and First Responders about their needs *before* engagement with industry.

In this context Australia needs a formally constituted national co-ordination body suitably financed and resourced to provide collaborative leadership, strategic oversight and policy direction to the evolution of the mission critical public safety communications ecosystem.

9.0 Advice to the Council of Australian Governments (Next Meeting is 9 February 2018)⁹

The policy and strategy context for Australian governments and subsequently COAG decisions relating to PSMB has changed significantly since the previous attempt to move forward with a PSMB capability for Australia's PSAs.

This change in policy and strategy context has been driven by a focus on national security, cyber threats, terrorism, domestic and community violence and violence against First Responders resulting from changes in public expectations and levels of confidence in Australian governments and their bureaucracies.

Previous and current Australian Government and Federal Department legislation, inquiries and announcements are now linked to the PSMB capability as follows:

- Next Generation Triple Zero Tender
- House of Representatives Standing Committee on Infrastructure, Transportation and Cities
 - 2016 report¹⁰ on the role of smart ICT in the design and planning of infrastructure
- The Australian Government's Security of Critical Infrastructure Bill
- The Australian Government's Telecommunications Sector Security Reforms Legislation
- The Australian Government's Home Affairs and Integrity Agencies Legislation Amendment Bill 2017
- The Australian Competition and Consumer Commission Domestic Mobile Roaming Declaration Inquiry
- The Australian Competition and Consumer Commission Australian Communications Study

Commentary about this changed policy context is provided in the following sections of this response:

- Next Generation Triple Zero Tender

⁹ <https://www.coag.gov.au/>

¹⁰ https://www.aph.gov.au/Parliamentary_Business/Committees/House/ITC/Smart_ICT/Report

The Australian Government has announced its intention to issue a Tender for a Next Generation Triple Zero Service incorporating Location Based Services (LBS) but no further information has been released. This decision was informed by a Discussion Paper issued by the Department of Communications and the Arts for comment through a public process. It is expected that the Next Generation Triple Zero Service will continue to be provided by a private sector organisation.

The current Triple Zero call service is a voice based component of the mission critical public safety communications ecosystem through which the public seeks assistance, reports incidents or provides information that requires a response from PSAs and First Responders. The Triple Zero Service transfers callers to nominated PSA Communication Centres for processing and response by First Responders using LMR and paging networks.

The *Next Generation* Triple Zero Service will be capable of receiving and transferring data (text, image, video, spatial and temporal etc.) to PSA Communications Centres which will then use the PSMB capability to transfer this data and any other related data to First Responders.

The importance of the Emergency Call Services and PSA Communications Centres¹¹ in the ecosystem has been progressively recognised through projects addressing the impact of PSMB on Communications Centres e.g. APCO International's Project 43¹², the National Emergency Communications Working Group (NECWG)¹³ White Paper and the establishment of the International Critical Control Rooms Alliance (ICCRA)¹⁴ by the TETRA and Critical Communications Association (TCCA) where the CDMPs is leading the ICCRA Operations Special Interest Group.

The direct connection between the Australian public, Next Generation Triple Zero Call Service, PSA Communications Centres, the PSMB capability and the services being delivered by PSAs and First Responders cannot be ignored from the perspective of interfacing, interoperability, training and cost needs to be provided in advice to COAG.

This direct connection also identifies the need for evidence based research into the "Fit for Purpose" assessment of existing PSA Communications Centres for both the *Next Generation* Triple Zero Call Service and the PSMB capability. This assessment should also address the current level of both intra State and cross border interoperability of PSA LMR networks.

- House of Representatives Standing Committee on Infrastructure, Transportation and Cities

The House of Representatives Standing Committee on Infrastructure, Transportation and Cities Committee's March 2016 report on the role of smart ICT in the design and planning of infrastructure has its origin in the 2014 inquiry by the former House Infrastructure and Communications Committee report into infrastructure planning and procurement.

The Standing Committee's report recommended to the Australian Government that public safety communications should be recognised as *mission critical infrastructure*.

¹¹ <http://www.policeforum.org/assets/EmergencyCommunications.pdf>

¹² <http://www.criticalcomms.com.au/content/public-safety/article/apco-releases-project-43-report-830588145#axzz52zR7p0Uo>

¹³ <http://necwg-anz.org/wp-content/uploads/2017/11/The-Emergency-Communication-Centre-of-the-Future-report-FINAL.pdf>

¹⁴ <http://www.iccraonline.com/iccra>

The Report also addressed a number of matters that will impact the mission critical public safety communications ecosystem in the future e.g. new technologies and applications such as Building Information Modelling (BIM), geospatial technology, the Internet of Things, machine learning, the importance of data collection to the development of smart infrastructure, open data and smart ICT—the need for data access, achieving compatibility of different data, devices and systems, harmonisation—national and international standards, data collection and storage capabilities and data security.

After nearly two years it appears that the Australian Government has not had the opportunity to consider this recommendation even though it has relevancy to the development of the PSMB capability and its treatment by Australian governments' as a major national infrastructure project.

- The Australian Government's Security of Critical Infrastructure Bill

On 23 January 2017 the Australian Government launched the Critical Infrastructure Centre which subsequently identified Australia's most critical infrastructure as being electricity, water, ports and *communications*.

The Security of Critical Infrastructure Bill 2017¹⁵ identifies the Australian *telecommunications systems and networks* are part of our national critical infrastructure and form the backbone for many other *critical infrastructure* sectors and services.

In October 2017 the Federal Attorney General announced that views were being sought on new legislation to help manage the complex and evolving *national security* risks from foreign involvement in Australia's *critical infrastructure*.

The government introduced the Security of Critical Infrastructure Bill 2017 to the Senate on 7 December 2017 to manage the complex and evolving *national security* risks of sabotage, espionage and coercion posed by foreign involvement in Australia's *critical infrastructure*.

The Bill was referred to the Parliamentary Joint Committee on Intelligence and Security¹⁶ with a report due by March 2018 *i.e. after advice is to be provided to COAG on the PSMB capability*.

- Telecommunications Sector Security Reforms Legislation

Communications as considered in the Security of Critical Infrastructure Bill 2017 has been transferred to the Telecommunications Sector Reforms Legislation which is due to become operational by September 2018. The Legislation introduces obligations on carriers and carriage service providers to do their best to protect networks and facilities from unauthorised access and interference.

Cyber security is a major risk for a PSMB capability because of the nature of the data the network will carry and the use to which it will be put by PSAs. In a service delivery model with a MNO as a commercial partner it should not be expected that PSAs will accept that a MNO will only have to do their best to protect its network from cyber or physical attack.

¹⁵ <http://criticalcomms.com.au/content/industry/article/canberra-reviews-critical-infrastructure-security-1039888649#ixzz52t4JmQd7>

¹⁶ https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bld=r6016

The level of protection needs to be addressed in conjunction with the Cyber Security Centre in the context of understanding the need for public safety grade cyber security infrastructure in the ecosystem and by comparison to the cyber security arrangements being included in international PSMB Projects.

- The Australian Government's Home Affairs Department

The Australian Government has announced its intention to establish a new of Home Affairs Department to form a super portfolio of *national security* Agencies keeping all Australians safe.

The Federal Government in previous iterations of PSMB capability has required provision be made for Agencies such as the Australian Federal Police and the predecessors of Australian Border Force. It is assumed that this requirement will remain in the current PSMB capability and therefore both the PSMB capability and the ecosystem needs to be identified as being linked to the new Home Affairs Department and that the Department will require its own specific service delivery model.

The Home Affairs and Integrity Agencies Legislation Amendment Bill 2017¹⁷ establishing the new Department has been referred to the Parliamentary Joint Committee on Intelligence and Security with a report due by February 2018.

- Australian Competition and Consumer Commission

The RFI notes that roaming or interconnection is an area of specific interest that should be addressed in RFI responses.

In October 2017 the Australian Competition and Consumer Commission (ACCC) concluded its public inquiry into whether to declare a domestic mobile roaming service announcing that it was not satisfied that the declaration would promote the long-term interests of end-users¹⁸.

However the ACCC's preliminary view was that the supply of a roaming service is technically feasible noting domestic and international commercial roaming arrangements that have been, or currently are, in place in Australia.

In a service delivery model with a MNO as a commercial partner the ability of PSAs to roam across Australia's commercial mobile networks to achieve the best level of coverage and capability relevant to the response to an incident would be a significant advantage. If PSAs confirm this roaming requirement its availability and cost should be discussed with the ACCC and included in PSMB capability contract negotiations.

In Europe Public Safety Communications Europe¹⁹ (PSCE) has identified the need for the review of European Union (EU) policy and regulation regarding mobile telecommunications, and the potential for infrastructure sharing for the delivery of mission critical applications/services, networks and devices on the basis that *no EU policy* currently identifies the need for critical mobile applications, networks and devices for operation and roaming across all European countries

¹⁷ https://www.accc.gov.au/system/files/Mobile%20roaming%20declaration%20inquiry%20final%20report_0.pdf

¹⁹ www.psc-europe.eu

- Australian Competition and Consumer Commission

The ACCC released its draft Report on the Australian Communications Study in October 2017.

This ACCC Study is relevant to the PSMB RFI because it addresses the makeup of the Sector, references the current commercial carriers (MNOs) likely to be considering their role in the PSMB capability and also the National Broadband Network (NBN).

The NBN is relevant to the mission critical public safety communications ecosystem because of its possible role in backhaul for the PSMBN and its progressive replacement of the ability for the public to use a direct line to contact the existing Triple Zero Call Service or an Emergency Information Line with a VoIP application. This concern is particularly relevant in high risk areas of Australia subject to natural disasters such as bushfires and flooding.

10.0 Use Cases in determining a PSMB Capability

The RFI does not reference any developed Use Cases to support the content in the RFI i.e. the absence of Use Cases developed and defined through a legitimate process of consultation and review inclusive of Australia's PSAs and First Responders (career professional and volunteer).

The PSMB RFI notes that because LMR networks for mission-critical voice communications do not support high data speeds mobile broadband use (by Australian PSAs) has been modest and primarily limited to non-mission-critical Use Cases due to concerns of the ability of commercial MNOs to reliably support mission-critical operations.

The RFI document also advises that Australian PSAs are seeking the same level of operational tools that many of their international peers are starting to utilise with their PSMB capabilities even though these capabilities are at various stages of maturity.

It would be unwise to consider that any commercial MNO fully understands the needs of Australia's PSAs and First Responders from a PSMB capability when Australia's PSAs and First Responders have not had the opportunity to participate in a national process to determine and document these needs in the form of Use Cases that would contribute to the development of a body of knowledge specific to Australia.

This approach contrasts with the approach taken by the international PSMB Projects where the focus has been on active on-going engagement with the public safety community to determine PSA and First Responder needs, collecting detailed data relevant to network design and engineering, application development and high quality independent research to specifically support mission critical public safety communications.

In the United States a partnership was developed between the FirstNet Agency (including a Public Safety Advisory Committee²⁰) (PSAC); the National Public Safety Telecommunications Council²¹ (NPSTC) which developed Position Papers describing the needs of PSA and First Responders and provided to the PSAC for endorsement for Use Case development²² and utilisation by the Public Safety Communications Research²³ (PSCR) Laboratories to produce outcomes incorporated in the

²⁰ <https://www.firstnet.gov/consultation/public-safety-advisory-committee>

²¹ <http://www.npstc.org/index.jsp>

²² <https://www.firstnet.gov/sites/default/files/PSAC%20Use%20Cases%20Report.pdf>

²³ <https://www.nist.gov/ctl/pscr>

development of the FirstNet Request For Proposal (RFP) and on-going research purposes related to the PSMB capability.

In the USA FirstNet had the benefit of being able to gather lessons learned from five LTE Early Builder Networks [Adams County, Colorado](#); [Los Angeles Regional Interoperable Communications System \(LA-RICS\), California](#); [New Jersey](#); [New Mexico](#) and [Texas](#) that were established to gather operational experience and specific lessons learned to assist in planning for the FirstNet PSMB network.

In Europe Public Safety Communications Europe (PSCE) invested heavily in consultation with a wide range of End Users in the BroadMap²⁴ Project to deliver a Final Definition of the Transition Roadmap and PCP Specification.

International practise is to develop public safety “Use Cases” to assist in standards development and/or the assessment of technologies and applications as being “fit for purpose” from a public safety communications perspective.

In Australia there has been no co-ordinated national effort to capture the outcomes and lessons learned from PSA use of commercial MNO networks for non-mission-critical use to assist in developing knowledge about the benefits available from a PSMB capability and the tools that need to be developed to capture these benefits.

11.0 Spectrum

Development of Business Models to support a PSMB capability have progressively moved away from providing a dedicated network built, owned and operated by PSAs, which was the traditional model used with LMR networks, to Business Models incorporating a MNO as a commercial partner.

International experience demonstrates that those countries preparing for or proceeding with the introduction of a PSBM capability have selected the 700MHz band for public safety communications use in conjunction with a MNO as a commercial partner.

The Australian Government recently completed the auctioning of all 700MHz spectrum for commercial use. This decision was consistent with its November 2016 decision to accept the recommendation by the Australian Productivity Commission that the least-cost option to provide Australia’s public-safety agencies with a PSMB capability is to use a commercial MNO carrier. This decision may have increased competition between carriers for the spectrum auction process knowing that they have Australian PSAs as potential locked-in customers needing a PSMB capability.

The Australian Communications and Media Authority (ACMA) has reserved 10 MHz (5+5) spectrum in the 800 MHz band for public safety communications. If PSAs wish to follow international PSMB capabilities and access 700MHz spectrum for the PSMB capability the MNO in a commercial partnership may charge a premium for this access covering both profit and revenue loss for the period of time that PSAs require access to 700 MHz spectrum.

The benefit from dedicated PSA spectrum to a MNO is captured when the MNO builds out the network to provide the PSMB capability to meet public safety grade requirements of higher resiliency and redundancy than that available through normal commercial MNO infrastructure.

²⁴ www.broadmap.edu

The MNO can then offer high value services to time and security sensitive commercial clients at a premium rate generating higher revenue to offset the cost of meeting the PSAs public safety grade requirements. The marketing value associated with the use of the MNO by PSA's should also not be under estimated.

While the Government has taken to opportunity generate revenue through the sale of spectrum and the ACMA has applied the concept of Opportunity Cost Pricing (OCP) to spectrum allocation and pricing the consequence of these actions and impact upon PSMB business and service delivery models has not been taken into account.

The ARCIA has been actively engaged with the ACMA on the application of OPC to spectrum for some time and in November 2014 produced a report²⁵ that determined the economic benefits of LMR spectrum use was between \$1.99 billion and \$3.72 billion per annum compared to an annual OCP of only \$39.7 million, indicating the benefits of LMR are at least 10 times greater than the next best alternative providing some indication of the value of PSA LMR networks.

12.0 Public Safety Apps

The international public safety community has identified the need for Public Safety Apps to meet the specific needs of PSAs and First Responders however the approach to providing these Apps has varied between countries.

In the United States APCO international established "Appcom" as a website at which App Developers could post applications thought to be relative to PSAs for comment but with no commitment to their "fit of purpose". This approach allowed APCO International to develop guidelines for Public Safety Apps.

In the United Kingdom Public Safety Apps require a formal accreditation as being fit for purpose for use on the British Telecom (BT) Network which provides the 999 Call Service. This accreditation process is conducted by British APCO.

FirstNet has now provided a dedicated portal²⁶ for App Developers to submit their Apps for review and certification on the basis that all Apps must explicitly demonstrate relevancy to Public Safety.

A current example of the civic infrastructure to support both public safety and non-public safety of applications is the Smart Street Lights²⁷ in San Diego.

Both the FirstNet and PSCE PSMB Objectives include the development of an Applications ecosystem.

The opportunity exists for the Australian public safety community to commence the development of specific public safety "Apps" for use in conjunction with the PSMB capability.

²⁵

<http://www.arcia.org.au/images/pdfs/Economic%20report%20on%20the%20value%20of%20LMR%20services%20in%20Australia.pdf>

²⁶ <https://developer.firstnet.att.com/firstnet>

²⁷ <https://spectrum.ieee.org/computing/it/san-diego-installs-smart-streetlights-to-monitor-the-metropolis>

13.0 PSMB Business Case

The RFI makes no reference to a Business Case to support the PSMB capability. It may be that the Productivity Commission Inquiry Report into PSMB released and accepted by the Australian Government in 2016 is considered a de-facto Business Case built on the recommendation to Government that using commercial mobile networks is the most efficient, effective and economical way of delivering a PSMB capability.

Clarification of the process to be used to develop a PSMB Business Case should be provided.

14.0 Transparency

The Discussion Papers released by the Federal Government and its Departments addressing *individual* components of the mission critical public safety communications ecosystem have one thing in common – public transparency.

The Parliamentary Joint Committee on Intelligence and Security Committee²⁸ is inviting public submissions on the legislative proposals referred to it.

Using the NSW Telco Authority as a vehicle to conduct an RFI process in conjunction with a restrictive timeframe to collect information from the telecommunications industry is not a transparent process for Australia's PSAs and First responders.

15.0 Consultation

In the USA FirstNet established an extremely strong regime of consultation – outreach with PSAs and First Responders from very early in the start-up phase of the Project.

The State of Texas²⁹ created a Public Safety Broadband Program supported by a website and created an online course³⁰ that provides background information on FirstNet and the nationwide PSMB Network. The on-line course highlighted some of the technology benefits that PSMB can bring for First Responders, and allowed comparison between PSMB and LMR.

There can be no doubt that the FirstNet consultation-outreach program has greatly contributed to all U.S. States agreeing to opt-in to the FirstNet – AT&T PSMB capability. Likewise in Europe Public Safety Communications Europe (PSCE) led a consultation-outreach program for the BroadMap Project funded by the European Commission.

Clarification about the consultation process for the PSMB capability needs to be provided for Australia's PSAs and First responders.

16.0 Public Safety Communications Roadmaps

The international PSMB Projects have all gone through an extensive planning process reflecting the degree of complexity and the need for extensive consultation and research to underpin Project documentation and process and to develop stakeholder management strategies.

²⁸ https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security

²⁹ <http://testing.txlte.com/>

³⁰ <http://testing.txlte.com/index.php/elearning-portal/>

Examples of these Roadmaps are as follows:

Also in the USA FirstNet produced Roadmaps³⁵ and used creative images as a key communication tool to inform its broad audience of stakeholders from Congress to First Responders a sample of which is provided in Figure No 3.

In Europe Public Safety Communications Europe (PSCE) produced a Transition Roadmap³⁶ for the European Union Interoperable Broadband and Communication Applications and Technology for Public Safety specification through a twelve month process of consultation with public safety representatives from 15 European Countries and NPSTC from the USA.



Figure No 3: FirstNet Roadmap

³⁴ <https://www.nist.gov/ctl/pscr/user-interface-user-experience-publications>

³⁶ https://www.psc-europe.eu/images/BMAP_FD_PR.pdf

17.0 Federated Capability

The use of a national Federated PSMB capability is both constitutionally consistent and aligned with current emergency management arrangements in Australia and emphasises the importance of the Ministerial Statement supporting the PSMB capability.

The use of a national Federated PSMB capability provides the governance and organisational opportunity to:

- Formally constitute a national co-ordination body to provide collaborative leadership, strategic oversight and policy direction to the evolution of the mission critical public safety communications ecosystem.
- Maintain jurisdictional management and control of the PSMB capability which when coupled with adherence to the use of open standards should remove the potential for cross border interconnection issues and interworking connection to LMR networks.
- Allow jurisdictions to consider the use of separate MNO or MVNOs with separate jurisdictional core(s) and access to the MNO or MVNOs RAN's as and when required.
- Allow jurisdictions to leverage investment in other LTE communication networks such as the transport sector and provide a higher level of network resilience and redundancy if a MNO has a major service disruption such as the Warrnambool telephone exchange fire³⁷ on 22 November 2012 as well as multiple other instances of MNO networks failing for various reasons.
- Allow the development of an Identification, Certification and Credential Management (ICAMS) Application to manage access by PSAs and First responders to the network as part of an overarching strategy for the security of critical infrastructure. The development of ICAMS as a national process would also support the movement of PSAs between jurisdictions for major incidents such as bushfires and floods.

Change management addressing organisational and cultural issues will need to be addressed as part of the PSMB capability consultation and planning process.

18.0 International Performance Measurement and Monitoring

The number of PSMB Projects now under way internationally offers the opportunity to compare the different approaches being taken to providing a PSMB capability. One such approach has been the publication of an index by Quixoticity³⁸ launched at the CommsConnect Conference in Melbourne in November 2017.

³⁷ <http://www.heraldsun.com.au/news/victoria/phone-lines-down-in-southwest-victoria-after-fire-at-warrnambool-telephone-exchange/news-story/fdc33fa7034c076666f71cc6a817a721?sv=bee0888956339a1225f24854bf1015b1>

³⁸ <https://www.quixoticity.com/>

This Index aims at identifying and promoting best practice in the world of public safety and critical communications and also references the United Nations Sustainable Development Goals (SDGs). Australia scored poorly³⁹ in the first edition of the new Index with the following comments being offered:

“Australia, Canada and Saudi Arabia could all be considered “smart followers”, actively opening up to many of the other nations in this Index. With strong governance, a diverse and active critical communications community and a willingness to learn from others, these 3 nations should be able to catch up with their global peers and show the way to many other nations yet to begin their journey.”

The United Nations special purpose agency, the International Telecommunications Union (ITU)⁴⁰, is also participating in the SDG by proposing indicators related to the contribution of information and communication technologies (ICT) including use of mobile phone networks and the internet towards achieving the SDGs by 2030. Realistically ICT has to include the PSMB capability of international PSAs and the University of Melbourne CDMPS has also commenced investigation into the linkages between the SDGs and disaster management and public safety which will link to mission critical public safety communications ecosystem.

19.0 The Sharing of Information and Research Outcomes

Illustrating the international collaboration now being seen within the public safety community is the PSCR sponsored research into the creation of a Mission Critical Open Platform (MCOP) which will benefit the whole public safety community by speeding up the commercial product release cycle, enabling new stakeholders to enter the public safety communications ecosystem and improve the awareness and common understanding of PSAs and both public safety industry and researchers of the mission critical suite of protocols.

The PSCR MCOP Research Project⁴¹ is funded by NIST being led by the University of the Basque Country⁴² and supported by the TCCA, Bittium and Expway⁴³

Looking to the future Collaborative Intelligent Transport Systems (C-ITS)⁴⁴ will form part of the mission critical public safety communications ecosystem with the PSMB capability allowing PSAs to integrate C-ITS in its future response capabilities to manage incidents that arise from consumer use of mobility as a service (MaaS) services and products e.g. autonomous vehicles.

The combination of the PSMB capability, C-ITS and MaaS will become linked to policy and strategy development relating to increased personal mobility e.g. the National Road Safety Strategy providing

³⁹ <http://criticalcomms.com.au/content/public-safety/article/australia-scores-poorly-in-international-index-714121661#ixzz53ifdApw2>

⁴⁰ <https://www.itu.int/en/ITU-D/Statistics/Pages/intlcoop/sdgs/default.aspx>

⁴¹ <https://www.nist.gov/ctl/pscr/mission-critical-open-platform>

⁴² <https://www.ehu.eus/en/en-home>

⁴³

https://www.nist.gov/sites/default/files/documents/2017/10/03/poster_universidad_del_pays_vascon_euskal_herriko_unibertsitatea_pdf.pdf

⁴⁴ <https://imovecsrc.com/>

governments, road authorities, police and other public safety officials significant opportunities to enhance the everyday safety of all Australians.

C-ITS will also will support the evolution of private and government sector initiatives like On Star⁴⁵ and eCall⁴⁶ which will also become part of the mission critical public safety communications ecosystem through their interfacing with future PSA Communication Centres and the PSMB capability.

The design of the proposed PSMB Proof of Concept needs to be robust enough take into account the impact of technology developments such C-ITS because by the time the PSMB capability is delivered and uniformly in use nationally many of the concepts mentioned as future developments will be in place.

20.0 Standards

Standards are developed by Standards Development Organisations (SDOs) which are commercial businesses relying heavily on relationships between industry (manufacturers and vendors), governments and their agencies to identify the need for Standards to support specific markets and sectors of those markets.

The public safety market is different to other markets as it deals with the lives, safety and security of individuals, communities and countries in an environment that has to deal with threats arising from both the natural and built environments varying in scale and occurrence but which universally rely on the mission critical public safety communications ecosystem to support PSAs and First Responders in the PPDR continuum.

Standards are therefore a critical component in the evolution of the mission critical public safety communications ecosystem and in particular the need for Open Standards to support operability and connectivity across the entire ecosystem.

The PSMB RFI appropriately states that Open Standards are to be applied to the PSMB capability and this approach needs to be maintained in all future steps to procure the capability for Australia's PSAs and First Responders.

Mission critical public safety SDOs are now focussing their efforts on the interconnection between LMR (P25 and TETRA) and LTE and commencing the discussion about the role of 5G in the context of the ecosystem.

Spatial Data Infrastructure

As previously stated at this point in time the PSMB capability is about the transport of "data" (text, images, video, spatial, temporal) and a large percentage of this data is expected to be spatially enabled or will become spatially enabled as part of utilising machine to machine learning and artificial intelligence in PSA functional applications and public safety "Apps" aimed at enhancing PSA and First Responder decision making.

The relevant Standards Development Organisation for spatial data is the Open Geospatial Consortium⁴⁷ (OGC) which is an international industry consortium of over five hundred companies,

⁴⁵ <https://www.onstar.com/us/en/home.html>

⁴⁶ https://ec.europa.eu/transport/themes/its/road/action_plan/ecall_en

⁴⁷ <http://www.opengeospatial.org/ogc>

government agencies and universities participating in a consensus process to develop publicly available interface standards.⁴⁸

The OGC has to be recognised as an SDO associated with the mission critical public safety communications ecosystem.

As part of the planning process to progress for the PSMB capability the level of participation by Australia in the development of the global Standards underpinning the mission critical public safety communications ecosystem should be reviewed.

21.0 PSMB RFI Time Frame

The time frame provided for the preparation of responses to the PSMB RFI was simply unrealistic e.g. 44 days (including weekends and the Christmas – New Year holidays or 28 business days) for industry to prepare and provide the raft of information being requested is not conducive to building trust into future relationships with governments on the PSMB Project.

One of the major risks of the unrealistic timeframe for responses to the PSMB RFI is that it will discourage serious consideration from any new entrant(s), particularly from outside Australia, to the public safety market and may even give the impression that there is already a pre-determined outcome from the process diminishing competition in the public safety market.

The restrictive PSMB RFI timeframe offers no incentive for responses to offer new features or capabilities which may be of interest to PSAs and meet the public safety grade requirements of the ecosystem.

Any new entrant(s) would be unlikely to propose building a new network solely to provide the PSMB capability however as a member of a consortium with a current MNO or a MVNO in a PPP focussed on long term investment in infrastructure could produce a different outcome.

Investment from international and local superannuation funds looking for potential for growth from infrastructure with a stable and growing customer base i.e. PSAs, providing new high value added innovative services capable of being utilised by other sectors may attract a new entrant to the market.

But it takes time to form such consortia and align strategy with broader government policy outcomes than just a PSMB capability.

22.0 Analysis of Q&A at the PSMB Industry Briefing

An analysis of questions and answers from the PSMB Industry Briefing held on 1 December 2017 identified the following themes:

- Time Frame
- Proof of Concept
- Next Steps
- Funding
- Network Size, Capability and Coverage
- State infrastructure availability
- Spectrum

These themes are consistent with the outcome of the gap analysis provided in this response to the PSMB RFI.

23.0 Conclusion

The matters raised in this response to the PSMB RFI are intended to positively reinforce the need for a PSMB capability as part of Australia's mission critical public safety communications ecosystem.

The Executive Summary included in the response summarises its outcomes by highlighting the risks and opportunities identified through the gap analysis.

Actions to address both the risks and opportunities are suggested in each section of the response.

The opportunities outweigh the risks and the risks are essentially process based and can be mitigated by government commitment as the PSMB RFI Ministerial Statement to "*enable law enforcement and emergency services to do what they do best – protect and help Australians in need*".

In support of the outcomes in this response it is recommended that:

- (a) As an outcome from the PSMB RFI evaluation process advice should be given to COAG that the mission critical public safety communications ecosystem should be recognised as *critical infrastructure* as recommended by the House of Representatives Standing Committee on Infrastructure, Transportation and Cities in 2016 *so that public safety communications can become part of the current boom in infrastructure investment by governments*.
- (b) The February time frame for advice to be provided to COAG on the outcomes from the PSMB RFI be extended to March to allow the Parliamentary Joint Committee on Intelligence and Security to consider the relationship between the PSMB capabilities and be addressed in the Committee's reports on the Home Affairs and Integrity Agencies Legislation Amendment Bill 2017 and the Security of Critical Infrastructure Bill which are due in February and March 2018 respectively.
- (c) The opportunity be taken as soon as possible to formally constitute a national co-ordination body to provide collaborative leadership, strategic oversight and policy direction to the evolution of the mission critical public safety communications ecosystem.

The public safety market is different to other markets as it deals with the lives, safety and security of individuals, communities and countries in an environment that has to deal with threats arising from both the natural and built environments varying in scale and occurrence but which universally rely on the mission critical public safety communications ecosystem to support PSAs and First Responders in the PPDR continuum.

For further information regarding this response to the PSMB RFI please contact:

Geoff Spring
Senior Industry Advisor
University of Melbourne
Centre for Disaster Management and Public Safety

Acronyms and Web Addresses		
ACCC	Australian Competition and Consumer Commission	www.accc.gov.au
ACMA	Australian Communications and Media Authority	www.acma.gov.au
APCO	Association of Public Safety Officials	www.apcointl.org
ARCIA	Australian Radio Communications Industry Association	www.arcia.org.au
ATCCF	Australian TETRA and Critical Communications Forum	http://www.criticalcommsforum.com.au/
BIM	Building Information Modelling	
BT	British Telecom	
CDMPS	Centre for Disaster Management and Public Safety	http://research.unimelb.edu.au/cdmgs
EU	European Union	
FWG	Functional Working Group	
ICCRA	International Critical Control Rooms Alliance	http://www.iccraonline.com/iccra
ICT	Information and Communications Technologies	
RFI	Request for Information	
LMR	Land Mobile Radio	
LBS	Location Based Services	
MNO	Mobile Network Operator	
MVNO	Mobile Virtual Network Operator	
NBN	National Broadband Network	
NECWG	National Emergency Communications Working Group	http://necwg-anz.org/
NPSTC	National Public Safety Telecommunications Council	http://www.npstc.org/index.jsp
OGC	Open Geospatial Consortium	http://www.opengeospatial.org/ogc
OPC	Opportunity Cost Pricing	
PPDR	Public Protection and Disaster Recovery	
PSAs	Public Safety Agencies	
PSAC	Public Safety Advisory Committee of FirstNet	https://www.firstnet.gov/consultation/public-safety-advisory-committee
PSCE	Public Safety Communications Europe	www.psc-europe.eu
PSCR	Public Safety Communications Europe - BroadMap	www.broadmap.edu
PSCR	Public Safety Communications Research	
PSMB	Public Safety Mobile Broadband	
TISN	Trusted Information Sharing Network	https://www.tisn.gov.au/Pages/default.aspx
RFP	Request For Proposal	
(SDOs)	Standards Development Organisations	
SOC	Senior Officers Committee	
TETRA	TETRA and Critical Communications Association	https://tcca.info/