2023 – 30 Australian Cyber Security Strategy

Discussion Paper

Submission from

University of Melbourne

Centre for Disaster Management and Public Safety
https://www.unimelb.edu.au/cdmps/home

in partnership with the Australian Radio Communications Association (ARCIA)

www.arcia.org.au

15 April 2023

1.0 Purpose:

The purpose of this Submission is to provide commentary on the 2023 – 2030 Australian Cyber Security Discussion Paper (the Discussion Paper) in the context of previous Submissions regarding the:

- Security Legislation Amendment (Critical Infrastructure) Bill 2020
  - The Bill amended the Security *of Critical Infrastructure Act 2018* to enhance the existing framework for managing risks relating to critical infrastructure;

- The statutory review of the *Security of Critical Infrastructure Act 2018*
  - An Act to create a framework for managing critical infrastructure, and for related purposes;

- The Review of Part 14 of the Telecommunications Act 1997 – Telecommunications Sector Security Reforms (TSSR)
  - The reforms established a regulatory framework to manage the national security risks of espionage, sabotage and foreign interference to Australia's telecommunications networks and facilities.

2.0 Introduction:

The University of Melbourne's Centre for Disaster Management and Public Safety (CDMPS) and its partners welcomes the opportunity to respond to the 2023 – 2030 Australian Cyber Security Strategy Discussion Paper and the questions listed for response in the Paper.

Strategic Intent

This Submission is consistent with the CDMPS's strategic intent to support multi-disciplinary collaboration between the research community, government, industry, and the community in delivering exceptional public safety outcomes in the context of the Mission Critical (Public Safety) Communications Ecosystem (the MCPSC Ecosystem).

Previous Submissions

Consistent with this strategic intent this Submission is one of several provided to various Australian Government Departments in particular the Department of Home Affairs Cyber and Infrastructure Security Centre (CISC) and the House of Representatives Committee on Infrastructure, Transport and Cities over past years seeking to have the MCPSC Ecosystem recognized as part of Australia's Critical Infrastructure and specifically part of the *"Communications" sector.*

The CDMPS Submission dated 12 February 2021 to the Parliamentary Joint Committee on Intelligence and Security (the Committee) review of the *Security Legislation Amendment (Critical Infrastructure) Bill 2020* in conjunction with the Statutory Review of the *Security of Critical Infrastructure Act 2018* and taking into consideration the Review of *Part 14 of the Telecommunications Act 1997 – Telecommunications Sector Security Reforms (TSSR)* has been attached to this Submission for reference purposes because its content and recommendations still remain relevant; to avoid

repetition of the advice provided in previous submissions; and to illustrate the industry partnerships that have substantially contributed to these Submissions and continue to do so.

Industry Partnerships and Support

Industry partners continually seek to raise awareness of the $4 Billion wireless communications sector that underpins the efficient operation of major infrastructure and public services in Australia. Without reliable communication technologies, communities cannot connect, industry will not grow, and economies will not prosper without the development of an innovative; sustainable and secure information and communications technology sector in Australia.

These industries act as gateway to a thriving international community of hundreds of global organizations committed to the sound evolution of an ecosystem that supports standardised critical communications for the professional users of these technologies. Collectively the focus of these industries has been to advocate for the use of standards based critical communications and harmonised spectrum and the principle of open and competitive markets to bring together market participants, users, suppliers, integrators and policy makers across our region and the world.

Therefore it is important to recognise that the wide range of industries and businesses associated with the broader Communications Sector are vitally interested in the development of the 2023 – 2030 Australian Cyber Security Strategy through partnerships such as the one with the CDMPS.

Utilising their commercial and industry expertise in the communications market these industries are willing to provide advice and guidance to government on all aspects of effectively managing the challenge of introducing rapidly evolving technologies that will benefit all Australians; while at the same time encouraging continuing significant private sector investment in these technologies; putting in place risk mitigation capabilities supported by appropriate legislative frameworks that will foster the upskilling and expertise of existing workforces; and the creation of resource pools with new skill sets to both grow technologies, encourage investment and provide the necessary protections expected by all Australians.

Legislative Recognition

The specific legislative recognition being sought by the CDMPS in this and previous submissions has progressively developed together with the technology evolution underpinning the MCPSC Ecosystem to suggest that the Ecosystem should now be recognised as a "System of National Significance (SoNS)" as per the amendment made on 2 April 2022 to the Security of Critical Infrastructure Act 2018 introducing a new enhanced cyber security obligations framework for systems of national significance —*Australia's most important critical infrastructure assets*.

Put in the simplest terms possible without this recognition of the MCPSC Ecosystem then Australia's Triple Zero system, being just one component of the total MCOSC Ecosystem, could be deemed as "non-critical" in times of emergency and/or natural disaster response and management.

3.0 Responses to Questions in The Discussion Paper

This Submission provides responses to questions 2a,2b,5,8,11,14,16,17, and 18 set out in the Discussion Paper as they relate specifically to the MCPSC Ecosystem.

For further simplification, these questions and their responses have been grouped under the broader headings of:

- Ecosystem Recognition
- Standards
- Procurement
- Operational

to demonstrate their linkages and need to be considered in the overall context of the Discussion Paper and its relationship to the MCPSC Ecosystem.

1. Ecosystem Recognition

Question 16:

It is noted that the Discussion Paper recognises the existence of specific "*ecosystems*" e.g. Australia's cyber security technologies *ecosystem*, as this is a good example of the terminology recognition which has been sort for several years in relation to the MCPSC Ecosystem. Cyber security will need to be considered a sub ecosystem in the context of new and emerging technologies such as the Public Safety Mobile Broadband Network (PSMB)[1], Next Generation Triple Zero system[2] (NG000) and the Internet of Public Safety Things (IoPST).

Cyber security needs to be examined through a technology lens and incorporated into government (Federal, State and Territory) policy and strategic planning processes that revolve around government, community, individual and commercially sensitive information e.g Personally Identifiable Information.

Question 17:

Future proofing of the MCPSC Ecosystem will require on-going investment by State and Territory Governments as current technologies require replacement, upgrading and introduction of new technologies such as PSMB and NG000 and most importantly *cyber security supported interoperability* and *encrypted* mission critical data transmission capabilities as they are introduced across the MCPSC Ecosystem.

The implementation of the recommendations from the Royal Commission into Australia's National Natural Disaster Management Arrangements arising from the 2019-20 Bushfires would be a significant step in assessing the existing capabilities and capacities of Australia's Public Safety Agencies and in particular the *stress testing* of these capabilities and capacities the results of which will provide guidance to *future proofing* of the MCPSC Ecosystem.

Noting that the Australian Government is currently considering the results of an independent PSMB Strategic Review commissioned in 2022 to determine the next steps to deliver this capability the opportunity exists to assess the future impact of the PSMB in the context of *stress testing* and *future proofing* the MCPSC Ecosystem and preparation for the introduction of NG000 at a future time.

[1] https://www.criticalcomms.com.au/content/public-safety/sponsored/australia-s-public-safety-poised-to-advance-with-shared-network-mobile-broadband-491800103

[2] https://www.criticalcomms.com.au/content/public-safety/article/next-generation-triple-zero-is-coming-618678434

Question 11:

The introduction of new technologies into the MCPSC Ecosystem should be expected to require the uplifting of cyber skills beyond the Government's broader STEM agenda. Australia's Public Safety Agencies and Emergency Management Sector will need to assess the additional level, source, timeframe, and investment for the procurement of these resources in what will be a competitive market. Given the nature of the MCPSC Ecosystem options such as partnering with other security sectors e.g. Defence and the development of a core set of resources with cyber security skill sets within the Sector and the broader Market will need to be considered.

2. Standards

Question 5:

The MCPSC Ecosystem needs to be underpinned by internationally developed, recognised, and applied open standards that encourage innovation and guide the form, design and cost of standards-based products and services to meet the future needs of individual markets and their sectors. Standards Development Organisations (SDOs) such as the 3GPP[3] perform this role bringing together manufacturers, sector representatives and government agencies. Australia needs to be represented in these SDOs as they move to address cyber security challenges through adoption of open standards.

Likewise Australia needs to be participating in research activities associated with the MCPSC Ecosystem through organisations such as NIST[4] and PSCR[5] and the Department of Homeland Security Critical Infrastructure and Security Agency (CISA)[6] in the USA. The testing of manufacturers products to ensure that they perform as per the standard and provide interoperability with other products is a critical part of the standards development process e.g Plug Tests[7].

This participation can be resource intensive and expensive but necessary investment to ensure that the MCPS Ecosystem keeps ahead of the evolving technology curve and the return on this investment should be captured by mandating the use of the standards across the MCPSC Ecosystem.

Question 2a:

Mandating the use of any "*operational"* standard across an Ecosystem, let alone one as important as cyber security with the impending rapid use of data through the introduction of new technologies needs to be "*transparent in the reasoning for the mandating to justify the investment"* required to meet the mandate.

Mandating will require consultation with industry and end users of the resulting products and services as well as a method of testing, recording, and reporting to ensure that the mandate is being applied and assessing its impact upon the Ecosystem i.e. the effective mitigation of operational cyber security risk and the flow on to the management of corporate risk in both commercial and government sectors.

[3] https://www.3gpp.org/
[44] https://www.nist.gov/cyberframework
[5] https://www.nist.gov/ctl/pscr
[6] https://www.cisa.gov/

[7] https://www.etsi.org/technologies/nfv/nfv-plugtests-programme

Where legislative reform is required there should be valuable "*Lessons Learned*" available from the consultation process conducted by the Department of Home Affairs Critical Infrastructure and Cyber Centre (CISC)[8] which supported the drafting of the SOCI Legislation.

Question 19:

Involvement in standards development provides the opportunity to become aware of emerging technologies; assess potential impacts and risk mitigation options that support *"security by design"* for input to policy and strategy development that avoids proprietary products and impedes interoperability within and across ecosystems.

Consultation with manufacturers, industry bodies and "End User" representative bodies throughout the design, development and deployment cycle will generate ownership of the design and risk mitigation in the operational use of technologies as well as provide input to next generation technologies.

3. Procurement

The use of "*procurement*" as a lever to increase cyber security is available to governments through the development and application of "*mandatory*" requirements around both products and services seeking to secure a place in the Australian public safety communications market and the MCPSC Ecosystem.

The use of mandatory requirements in conjunction with the removal of proprietary barriers in procurement processes would assist in the development of an open competitive marketplace through which governments can seek to purchase best value products and services with built in cyber security and risk-based mitigation capabilities.

In the case of the MCPSC Ecosystem the involvement of "End User" input should also be considered essential because of the reliance of First Responders on the Ecosystem and its components for their occupational health and safety.

4. Operational

Question 8:

Given the important role performed by Australia's Public Safety Agencies in protecting our population, its communities, and businesses the existence of a specific "*obligation of confidentiality*" between the Australian Signals Directorate[9] (ASD) and organisations subjected to cyber security breaches would seem to be appropriate particularly in the response and mitigation phases of an attack.

This obligation of confidentiality should also be extended to Public Safety Agencies who become victims of cyber security incidents such as the incident involving Fire Rescue Victoria[10] and the on-

[8] https://www.cisc.gov.au/
[9] https://www.asd.gov.au/
[10] Update on FRV cyber-attack 11 January 2023

going investigation and resolution of the incident. The involvement of regulators investigating incidents could from part of the post incident review which is the subject of Question 14.

Question 14:

Public Safety Agencies have a well-established model for post incident reviews and large commercial organisations would be expected to have similar models which could also be modified.

The development of a specific model for cyber security incidents including participation by Regulators should be facilitated with industry and other key stakeholders and impacted parties to produce post incident action reports that may make recommendations that modify and improve responses too and management of cyber security incidents.

Question 2b:

It appears that with the call for submissions regarding the development of a "2023 – 2030 Australian Cyber Security Strategy" the reform of the Security of Critical Infrastructure Act is already under consideration and therefore it is an opportunity to once again put forward the position that the MCPSC Ecosystem should be recognised in legislation as "*Critical Infrastructure*".

As indicated in the selection of questions responded to in this Submission the MCPSC Ecosystem will only become more complex with the incorporation of new technologies to meet public expectations of the quality of responses by Public Safety Agencies to requests to the Triple Zero service for assistance in individual emergencies or as part of a broader responses to natural hazards and disasters.

This increasing complexity should result in the MCPSC Ecosystem being recognised as a *"System of National Significance"* as provided for in the existing Legislation and in any further reform of the legislation.

4.0 Contact for information relating to this Submission:

Geoff Spring – Honorary Fellow - Senior Industry Advisor

University of Melbourne - Centre for Disaster Management and Public

Safety Mission Critical Communications Research Unit

[redacted]

[redacted]

Attachment To:

2023 – 30 Australian Cyber Security Strategy

Discussion Paper – 15 April 2023

REVIEW OF THE SECURITY LEGISLATION AMENDMENT (CRITICAL INFRASTRUCTURE) BILL 2020 AND STATUTORY REVIEW OF THE SECURITY OF CRITICAL INFRASTRUCTURE ACT 2018

(taking into consideration the Review of *Part 14 of the Telecommunications Act 1997 – Telecommunications Sector Security Reforms (TSSR)*

Submission from

University of Melbourne

Centre for Disaster Management and Public Safety

https://www.unimelb.edu.au/cdmps/home

12 February 2021

In Conjunction with

Australian Critical Communications Forum https://criticalcommsforum.com.au/

Australian Radio Communications Industry Association https://arcia.org.au/

REVIEW OF THE SECURITY LEGISLATION AMENDMENT (CRITICAL INFRASTRUCTURE) BILL 2020 AND STATUTORY REVIEW OF THE SECURITY OF CRITICAL INFRASTRUCTURE ACT 2018

taking into consideration the Review of *Part 14 of the Telecommunications Act 1997 – Telecommunications Sector Security Reforms (TSSR).*

1.0 Purpose:

The purpose of this Submission is to provide commentary on;

- Security Legislation Amendment (Critical Infrastructure) Bill 2020 ○ The Bill amends the Security *of Critical Infrastructure Act 2018* to enhance the existing framework for managing risks relating to critical infrastructure;

- The statutory review of the *Security of Critical Infrastructure Act 2018* ○ An Act to create a framework for managing critical infrastructure, and for related purposes;

- The Review of Part 14 of the Telecommunications Act 1997 – Telecommunications Sector Security Reforms (TSSR)

  ○ The reforms established a regulatory framework to manage the national security risks of espionage, sabotage and foreign interference to Australia's telecommunications networks and facilities.

2.0 Introduction:

The University of Melbourne's Centre for Disaster Management and Public Safety (CDMPS)[11] welcomes the opportunity to respond to the Parliamentary Joint Committee on Intelligence and Security (the Committee) review of the *Security Legislation Amendment (Critical Infrastructure) Bill 2020* in conjunction with the Statutory Review of the *Security of Critical Infrastructure Act 2018* and taking into consideration the Review of *Part 14 of the Telecommunications Act 1997 – Telecommunications Sector Security Reforms (TSSR).*

The CDMPS is making this Submission in conjunction with the following industry partners:

- Australian Radio Communications Industry Association (ARCIA)[12]

[11] http://research.unimelb.edu.au/cdmps
[12] www.arcia.org.au

- Australian Critical Communications Forum (ACCF)[13]
- Australian Control Room Network Association (ACRNA)[14]

in the context of their respective roles in the critical communications sector and in particular the *mission critical (public safety) communications Ecosystem (the Ecosystem)* and the role it performs both routinely and in times of natural disasters and pandemic such as we are experiencing at the present time.

This Submission is consistent with the CDMPS's strategic intent to support multi-disciplinary collaboration between the research community, government, industry, and the community in delivering exceptional public safety outcomes in the context of the Mission Critical (Public Safety) Communications Ecosystem (the Ecosystem).

This Submission is one of several provided to various Australian Government Departments and the House of Representatives Committee on Infrastructure, Transport and Cities over past years seeking to have the Ecosystem recognized as part of Australia's Critical Infrastructure and specifically part of the *"Communications" sector.*

3.0 Summary

The following is a Summary of the advice provided in this Submission:

- The Mission Critical (Public Safety) Communications Ecosystem needs to be recognized as part of Australia's Critical Infrastructure and specifically part of the *Communications Sector* within which it should be treated as a *System of National Significance.*

- The CDMPS Submission in January 2018 provided support for the Security of Critical Infrastructure Bill 2017 - *A Bill for an Act to create a framework for managing critical infrastructure, and for related purposes* and referenced the TSSR. The basis for that support of the Framework remains relevant to-day and should benefit from being considered in the current review of the proposed legislation.

- The proposed legislation should be developed into a fully integrated suite of legislation to keep pace with the evolution of technology across the expanded sectors of Critical Infrastructure.

- The review of the proposed legislation should take into consideration the recommendations made by Royal Commission *into Australia's National Natural Disaster Management*
  Arrangements' specific to critical infrastructure.

- The proposed legislation needs to recognise the growing attractiveness of the communications sector and its infrastructure assets to private sector investment and its potential participation in the Ecosystem.

[13] https://criticalcommsforum.com.au/
[14] https://acrna.org/

- The significant cultural and organizational change within Australia's PSAs that will need to be addressed in conjunction with the introduction of the PSMB capability; the evolution of the Ecosystem; and the associated security obligations of Critical Infrastructure more broadly.

4.0 Critical Infrastructure - Definition

In the period from 2015 to the present time the definition of "Critical Infrastructure" emerged in legislation and continued to evolve in parallel with the evolution of the Ecosystem as it continues to transition from analogue to digital technologies.

The establishment of the Critical Infrastructure Centre[15] (CIC)within the Department of Home Affairs (DHA) has seen the statement about critical infrastructure shown below adopted and used in subsequent policy development regarding what constitutes Australia's Critical Infrastructure leading into other related matters such as cyber security which has been considered in a policy sense with the release on 6 August 2020 of Australia's Cyber Security Strategy 2020[16].

"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".*

This Submission utilises this definition of Critical Infrastructure as a component of the National Disaster Risk Reduction Framework[17] in conjunction with the DHACIC *Protecting Critical Infrastructure and Systems of National Significance* Consultation Paper which noted that *''all Australians rely on critical infrastructure to deliver essential services that are crucial to our way of life such as communications''* positioning the Ecosystem within the category of *Systems of National Significance* given the applicable Description and Framework Elements described in the Consultation Paper.

5.0 Prior Submissions

January 2018:

The CDMPS made a Submission to the Committee regarding the Security of Critical Infrastructure Bill 2017 - *A Bill for an Act to create a framework for managing critical infrastructure, and for related purposes* and referenced the TSSR.

[15] https://cicentre.gov.au/

[16] https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf

[17] https://www.homeaffairs.gov.au/emergency/files/national-disaster-risk-reduction-framework.pdf

The Security of Critical Infrastructure Bill 2017 transferred *telecommunications* to the TSSR Legislation which became operational in September 2018. The TSSR Legislation introduced obligations on carriers and carriage service providers to *do their best* to protect networks and facilities from unauthorised access and interference.

The CDMPS Submission in January 2018 provided the following commentary:

"From perspective of the mission critical public safety communications ecosystem and its mission critical applications/services, networks, and devices the Security of Critical Infrastructure Bill 2017, TSSR Legislation and other supporting legislation e.g. The Telecommunications Interception Act, need to be jointly applied to effectively ensure a "fit for purpose" environment able to accommodate; increasing private sector participation; the carriage of sensitive data as well as voice communications; and public confidence in and expectations of Australia's Public safety Agencies (PSAs) and national security agencies".

It is suggested that this commentary remains relevant to-day and needs to be considered in the current review of the proposed legislation with a view to the development of a fully integrated suite of legislation to keep pace with the evolution of technology across the expanded sectors of Critical Infrastructure as currently proposed.

The CDMPS Submission also suggested opportunities for the Australian Government to align the Ecosystem with the Framework to be created by the Security of Critical Infrastructure Bill 2017 to manage risks to national security relating to critical infrastructure. The CDMPS Submission therefore supported the Framework based on the following:

- The process of developing the Security of Critical Infrastructure Bill 2017 clearly established the relationship between telecommunications, (*systems and networks)* as national critical infrastructure and national security.

- The mission critical public safety communications ecosystem and the proposed Public Safety Mobile Broadband (PSMB) capability needed to be linked to the new Home Affairs Department and the national security agencies within the Department.

- Australia's Public Safety Agencies (PSAs) and national security agencies *should not be expected* to accept in any PSMB service delivery model incorporating a commercial carrier where the TSSR requirement is that the commercial carrier will only have to *do their best* to protect its network from cyber or physical attack.

- In any PSMB service delivery model the ability of Australia's PSAs and national security agencies to roam across Australia's commercial mobile networks to achieve the best level of coverage and capability relevant to the response to an incident or investigation would be a significant advantage[18].

[18] *Note: The ACCC's inquiry into the need for a domestic mobile roaming service expressed a preliminary view 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.*

- PSA and national security agencies confirmation of a mobile roaming requirement would add another layer of complexity to the cyber security environment for the mission critical public safety communications ecosystem.

- Cyber security for the evolving mission critical public safety communications ecosystem will also need to be robust enough to consider the impact of technology developments such as Collaborative Intelligent Transport Systems (C-ITS)[19] 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.

- The linking of the Security of Critical Infrastructure Bill 2017 to the TSSR and other supporting Legislation relating to critical infrastructure will enhance the ability to manage risks to national security and provide a base for determining the level of cyber security protection required for the evolving mission critical public safety communications ecosystem.

- The Critical Infrastructure Centre should work with Australia's PSAs and national security agencies to develop Use Cases, taking into consideration cyber security arrangements included in international PSMB Projects, to guide the development of a public safety grade cyber security environment to protect the evolving mission critical public safety communications ecosystem.

Three Years on from providing the above advice in support of the Framework there has been little progress in progressing the PSMB capability, other than the release of a Request for Proposals for a Proof of Concept. However, the advice previously provided remains relevant as the Royal Commission found that the PSMB component of the Ecosystem is *a widely recognized gap in the communications platforms available to Australia's First Responders*[20]. The CDMPS and its industry partners (ARCIA, ACCF and ACRNA) therefore remain strong supporters of a PSMB capability as referenced in the findings of the Productivity Commission Research Report[21] into PSMB delivered in December 2015

28 April 2020:

The CDMPS made a Submission[22] to the *Royal Commission into Australia's National Natural Disaster Management Arrangements* which made the following recommendations:

(a) The Australian Government formally recognise in legislation Australia's mission critical (public safety) communications Ecosystem as Critical Infrastructure;

(b) The Australian Government formally recognise in legislation the role of the Ecosystem in providing an essential service[23] *to Australia's Public Safety Agencies supported by*

[19] https://imovecrc.com/

[20] *(refer Paragraph 125 of the Commission's Initial Observations publication).*

[21] https://www.pc.gov.au/inquiries/completed/public-safety-mobile-broadband/report

[22] https://naturaldisaster.royalcommission.gov.au/system/files/2020-07/NND.600.00246.pdf

[23] "Essential services" in the context of this report means services, by whomsoever rendered and whether rendered to the government or to any other person, the interpretation of which would endanger the life, health or personal safety of the whole or part of the population.

specialist industries and supply chains functioning efficiently and competitively in an internationally standards based public safety market.

(c) The Australian Government provide a legislative, regulatory, governance and administrative framework within a federated national model to facilitate; the seamless operation of the Ecosystem; enabling its effective contribution to the delivery of public safety outcomes meeting the expectations of all Australians; while protecting the health and wellbeing of Australia's First Responder community[24].

(d) The Australian Government initiates the development of a whole of Ecosystem RoadMap underpinned by a systems approach for use in consultative processes with Key Stakeholders facilitating the transparent monitoring and reporting of the evolution of the Ecosystem.

(e) The Australian Government initiate a national "Fit for Purpose" assessment of existing Public Safety Agency Communications Centres for both current and future connectivity with; the Next Generation Triple Zero Call Service; existing and planned Land Mobile Radio (LMR) networks; and the proposed Public Safety Mobile Broadband (PSMB) capability including both intra State/Territory and cross border interoperability.

In making these recommendations to the Commission it is recognised that there will be significant hurdles to be overcome in the co-ordination of the consideration of the recommendations across the many channels of bureaucracy at Federal and State/Territory level however in the era of reform coming out of the current pandemic crisis and in the context of the need for preparation for the 2020 – 21 and future Fire Seasons there should be an attempt to capture this significant opportunity."

These recommendations remain relevant today and would be supported by the proposed legislation currently being reviewed by the Committee.

<u>27 November 2020:</u>

The CDMPS provided a Submission responding to the previously referenced Department of Home Affairs – Critical Infrastructure Centre (DHACIC) *Protecting Critical Infrastructure and Systems of National Significance Exposure Draft Security Legislation Amendment (Critical Infrastructure) Bill 2020.*

The Submission highlighted the need to consider the recommendations contained in the Final Report of the *Royal Commission into Australia's National Natural Disaster Management Arrangements* that are linked to the Ecosystem and Australia's Critical Infrastructure (refer to Section 9.0 of this Submission) and hence the need to address these recommendations in the context of the proposed legislation being reviewed by the Committee.

[24] Police, Fire, Ambulance and State Emergency Services, Lifesaving Australia, and Australia's National Security Agencies

6.0 Ecosystem Components – Legislative Recognition and Protection

The initial drive to have the Ecosystem recognised as critical infrastructure came from a proposal to provide a PSMB capability for Australia's Public Safety and Law Enforcement Agencies which, as currently proposed, will use the *telecommunications* networks of Australia's Mobile Network Operators (MNOs) as per the current categorisation of critical infrastructure, to provide a dedicated voice and data (location, video, etc) service using network technologies (Priority, Pre-emption and Quality of Service – PPQoS) in conjunction with use of a Mobile Virtual Network Operator (MVNO). The evolutionary nature of telecommunications networks and associated systems and the capacity to transmit high data volumes in real time will see an increased adoption and reliance by communities, businesses and PSAs that will demand high levels of reliability, guaranteed levels service and resilience. Quality voice, data and video will become the expected and accepted norm.

PSMB capabilities are currently being provided in the United States by AT&T in partnership with the FirstNet[25] Agency and in the United Kingdom by the Home Office Emergency Services Network[26] (ESN) in conjunction with mobile network operator EE. Europe is proceeding with the BroadWay Project to deliver a pan-European PSMB capability [27]while New Zealand has just released a Request for Proposals for a new Public Safety Network[28] that will provide a PSMB capability in conjunction with a new Land Mobile Radio (LMR) Network.

Land Mobile Radio (LMR) networks provide high quality voice communications for both strategic and tactical communications and provide resilience (mission critical voice and thin data) to the *Ecosystem* when commercial *telecommunications* infrastructure fails.

It is now recognised that the LMR and PSMB components of the Ecosystem are compatible and not substitutional and investment in both will be required into the future such as the Federal Government's STAND[29] Program announced in May 2020. New South Wales, Tasmania and Western Australia have all announced extensions of existing networks or new LMR networks.

The introduction of PSMB into the Ecosystem will bring *telecommunications and radio communications together* i.e. Land Mobile Radio (LMR) and Long-Term Evolution (LTE) technologies, using their respective international standards and utilising the interworking currently under development that will facilitate interoperability.

The Next Generation Triple Zero platform will provide the ability to receive data associated with Triple Zero calls in addition to voice and the ability using *telecommunications* networks to transfer both voice and data to PSA Communication Centres which will be connected to both LMR and LTE Networks.

---

[25] https://www.firstnet.gov/

[26] https://www.gov.uk/government/publications/the-emergency-services-mobile-communicationsprogramme/emergency-services-network

[27] https://www.broadway-info.eu/

[28] https://www.publicsafetynetwork.nz/

[29] https://minister.infrastructure.gov.au/littleproud/media-release/hundreds-satellite-dishes-give-betterbroadband-connectivity-during-natural-disasters

While the initial focus has been on the PSMB what cannot be ignored is the need to recognise the entire *Ecosystem* as Critical Infrastructure and that the Ecosystem will continue to evolve and expand with the introduction of new technologies and services e.g. satellite networks and the Internet of Public Safety Things[30] (IoPSTs) resulting in the Ecosystem becoming increasingly interconnected and vulnerable to disruption from both natural and human interventions.

This evolution will need the Ecosystem to be protected by appropriate legislation to effectively manage increasing private sector participation and external risks such as cyber security, supply chain and energy continuity risks

7.0 Inquiries into the 2019-20 Bushfires

Published Reports from Inquiries into the 2019-2020 Bushfires have been examined for their relevance to the Ecosystem and to determine their focus and guidance as to where investment is required in both its current and evolved form.

This initial examination has revealed mid-range mention of critical infrastructure and no mention of cybersecurity, either in conjunction with critical infrastructure or as a standalone item illustrating the significant cultural and organizational change within Australia's PSAs that will need to be addressed in conjunction with the introduction of the PSMB capability; the evolution of the Ecosystem; and the associated security obligations of Critical Infrastructure more broadly.

8.0 The Implications of "Data"

The introduction of data into the Ecosystem will need to be considered in legislation to ensure that it is appropriately managed and protected e.g. as previously referenced the Next Generation Triple Zero service will enable both voice and data-based requests for emergency assistance requiring the generation and carriage of data through the Ecosystem. In this process the initial data received may be enhanced by accessing a range of data bases or data being supplied by other technologies such as the Internet of Public Safety Things and/or the sharing of data between PSAs for use in operational response which may trigger Consumer Data Right protections as microeconomic reform through its extension to the *telecommunications* sector.

9.0 Royal Commission into Australia's National Natural Disaster Management Arrangements

The Final Report of the Royal Commission into Australia's National Natural Disaster Management Arrangements made 80 Recommendations to the Commonwealth Government all of which have been accepted by the Government and are under consideration by Australia's States and Territories.

Examination of these 80 recommendations for their relevance to the Ecosystem has identified 27 Recommendations, 19 as Core Recommendations and eight as Supporting

30 https://www.npstc.org/download.jsp?tableId=37&column=217&id=4195&file=NPSTC_PSIoT_Use_Cases_Repo rt_190616.pdf

Recommendations. A full summary of these Recommendations is provided as an Attachment to this Submission.

Within these 27 Recommendations Chapter 9: Essential Services provides references to *Critical Infrastructure* in Recommendations 9.4 and 9.5 as follows:

- Chapter 9: Essential services

  - Recommendation 9.4: Collective awareness and mitigation of risks to critical infrastructure

    The Australian government, working with state and territory governments and critical infrastructure operators, should lead to a process to:

    - Identify critical infrastructure;
    - Assess key risks to identify critical infrastructure from natural disasters of national scale or consequence;
    - Identify steps needed to mitigate these risks;
    - Identify steps to make critical infrastructure more resilient;
    - Track achievement against an agreed plan.

  - Recommendation 9.5: Improving coordination between critical infrastructure sectors and with government.

    The Australian government should work with state and territory governments and critical infrastructure operators to improve information flows during and in response to natural disasters:

    - between critical infrastructure operators
    - between critical infrastructure operators and government

The review of the legislation should take into consideration the Royal Commission's specific recommendations regarding critical infrastructure.

10.0 Private Sector Investment in the Communications Sector

The growing attractiveness of the communications sector and its infrastructure assets to private sector investment is illustrated by current interest in the communications towers that are an integral component of communication networks. Communication towers owned by Australian MNOs Telstra's InfraCo, and Optus are both being readied for sale while similar sales have been undertaken in the USA.

Communication towers are part of the Ecosystem therefore this tend illustrates the need to have the ownership of communication towers and associated infrastructure assets addressed in the proposed Legislation to protect the Ecosystem.

11.0 Contact for information relating to this Submission:

Geoff Spring - Senior Industry Advisor

University of Melbourne - Centre for Disaster Management and

Public Safety Mission Critical Communications Research Unit

[redacted]

Attachment:

REVIEW OF THE SECURITY LEGISLATION AMENDMENT (CRITICAL INFRASTRUCTURE) BILL 2020 AND STATUTORY REVIEW OF THE SECURITY OF CRITICAL INFRASTRUCTURE ACT 2018 Royal Commission Inquiry into Australia's National Natural Disaster Arrangements

Recommendations considered relevant to the Mission Critical (Public Safety) Communications Ecosystem (Core and Supporting)

Preliminary analysis of the Royal Commission's recommendations to the Commonwealth Government and the Commonwealth Government's response has identified the following Core and Supporting recommendations for further examination:

1. Core Recommendations

✞ **Chapter 3: National coordination arrangements:**

- Recommendation 3.1: **Forum for Ministers** – restructure and reinvigorate ministerial forums with a view to enabling timely and informed decision making.

- Recommendation 3.2: Establishment of an authoritative disaster advisory body – **to consolidate advice *on strategic policy and operational considerations* for Ministers**

- Recommendation 3.6: Establishing a standing resilience and recovery entity - …**building on the responsibilities of Emergency Management Australia** to include facilitating resource adhering decisions of governments and ***stress testing*** national disaster plans

✞ **Chapter 4 Supporting better decisions**

- Recommendation 4.1: National Disaster risk information - …implementation of ***harmonized data* governance** and ***national data standards***

- Recommendation 4.2: Common information platforms and shared technologies – create ***common information platforms and share technologies to enable collaboration*** in the production of, analysis, access and exchange of information, data, and knowledge….

- Recommendation 4.4: Features of the National Disaster Risk Information Services Capability - … should include **tools and systems to support operational and strategic decision making**…to meet the various ***needs*** of relevant industry sectors and end users

- Recommendation 4.6: Consistent impact ***data standards*** – Australian, state and territory governments should ***work together to develop consistent data standards to measure***….

✞ **Chapter 6: National emergency response capability**

- Recommendation 6.1: ***Assessment of the capacity and capability of fire and emergency services*** in light of current and future natural disaster risk.

- Recommendation 6.2: A national register of fire and emergency services personnel and equipment.

- Recommendation 6.3: ***Interoperable communications*** for fire and emergency services ***across jurisdictions***

- Recommendation 6.4: ***Delivery of a Public Safety Mobile Broadband capability***

- Recommendation 6.5: Multi-agency national-level exercises

✞ **Chapter 8: National aerial firefighting capabilities and arrangements**

Recommendation 8.1: ***A sovereign aerial firefighting capability*** ○

Recommendation 8.2: ***Research and evaluation into aerial firefighting***

- Recommendation 8.3: Developing the aerial firefighting industry's capability

✞ **Chapter 9: Essential services**

- Recommendation 9.1: Supply chains – government review – review ***supply chain risks***

- Recommendation 9.3 Provision of information - …information should be provided in ***real time or in advance based upon predictions where possible.***

- Recommendation 9.4: Collective awareness and mitigation of risks to critical infrastructure

The Australian government, working with state and territory governments ***and critical infrastructure operators,*** should lead to a process to:

- Identify critical infrastructure
- Assess key risks to identify critical infrastructure from natural disasters of national scale or consequence
- Identify steps needed to mitigate these risks
- Identify steps to make critical infrastructure more resilient – *relates to public safety grade* • Track achievement against an agreed plan

- Recommendation 9.5: ***Improving coordination between critical infrastructure sectors*** and with government.

The Australian government should work with state and territory governments and ***critical infrastructure operators*** to improve information flows during and in response to natural disasters:

- **between *critical infrastructure operators***

- **between *critical infrastructure operators and government***

2. Supporting Recommendations

✞ Chapter 5: Declaration of a national emergency

○ Recommendation 5.1: Make provision for a declaration of a state of emergency: - relates to Critical Infrastructure and Cyber Security i.e.

- Ability to make a Declaration
- Processes to mobilise and activate
- The power to take action

✞ Chapter 7: Role of the Australian Defence Force

○ Recommendation 7.1: Improve understanding of Australian Defence Force capabilities

○ Recommendation 7.2: Review of Defence Assistance to the Civil Community

✞ Chapter 11: Emergency Planning

○ Recommendation 11.2: Resource sharing arrangements between local governments State and Territory Governments should review their arrangements for sharing resources between their local governments during natural disasters, including whether these arrangements provide sufficient ***surge capacity***

✞ Chapter 13: Emergency Information and Warnings

○ Recommendation 13.5 The development of national standards for mobile applications – develop minimum ***standards*** of information to be included in bushfire warning apps

✞ Chapter 15: Health

○ Recommendation 15.3: Prioritizing mental health during and after natural disasters

…develop consistent and compatible methods and metrics health impacts related to natural disasters, including mental health and take steps to ensure the appropriate *sharing of health and mental health databases.*

✞ Chapter 17 Public and private land management

○ Recommendation 17.1: Public availability of fuel load management strategies, including the rationale behind them.

✞ Chapter 22 Delivery of recovery services and financial assistance

○ Recommendation 22.2: **Appropriate sharing of personal information** take account of all necessary safeguards to ensure the sharing is only for recovery purposes.