Department of Home Affairs – Critical Infrastructure Centre

Submission

Protecting Critical Infrastructure and Systems of National Significance

Exposure Draft Security Legislation Amendment (Critical Infrastructure) Bill 2020

27 November 2020

In Conjunction with

Australian Critical Communications Forum	https://criticalcommsforum.com.au/
Australian Radio Communications Industry Association	https://arcia.org.au/
Australian Control Rooms Network Association	https://acrna.org/
Centre for Disaster Management and Public Safety	https://www.unimelb.edu.au/cdmps/home

Department of Home Affairs – Critical Infrastructure Centre

27 November 2020

Protecting Critical Infrastructure and Systems of National Significance

Exposure Draft Security Legislation Amendment (Critical Infrastructure) Bill 2020

Purpose:

The purpose of this submission is to provide additional information to that contained in a previous submission made by the University of Melbourne Centre for Disaster Management and Public Safety (CDMPS) to the Department of Home Affairs – Critical Infrastructure Centre (DHACIC) on 16 August 2020 which responded to the Consultation Paper - *Protecting Critical Infrastructure and Systems of National Significance* dated 12 August 2020. Included with the original submission was a copy of a submission made by the CDMPS and its industry partners to the *Royal Commission into Australia's National Natural Disaster Management Arrangements* which should be referred to in considering this submission.

The original submission noted that:

- The submission to the Commission was one of several provided over past years to various Australian Government Departments and the House of Representatives Committee on Infrastructure, Transport and Cities seeking to have the Mission Critical (Public Safety) Communications *Ecosystem* recognized as part of Australia's Critical Infrastructure and specifically part of the *"Communications" sector; and*

- In the context of the *Protecting Critical Infrastructure and Systems of National Significance* Consultation Paper it would appear that the *Ecosystem* falls within the category of *Systems of National Significance* given the applicable Description and Framework Elements shown in Figure 1 in the Consultation Paper.

Discussion:

As noted in the DHACIC Consultation Paper *''all Australians relay on critical infrastructure to deliver essential services that are crucial to our way of life such as communications''*. This statement supports the *Ecosystem* being considered as a subset of the Critical Infrastructure "communications sector "and like the sector itself the *Ecosystem* is becoming increasingly interconnected and interdependent as new components of the *Ecosystem* are added and others enhanced in their capacity and capability.

- Royal Commission Recommendations related to the *Ecosystem*

The Royal Commission's Final Report into Australia's National Natural Disaster Management Arrangements also highlighted the dependence of Australians on critical infrastructure and made linked recommendations that relate to the *Ecosystem* hence also supporting the *Ecosystem* being considered as a subset of the Critical Infrastructure "communications sector ".

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

State and territory governments:

- Should have a structured process to regularly assess the capacity and capability requirements of fire and emergency services, in light of both current and future natural disaster risk.

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

State and territory governments:

- Should update and implement the National Framework to Improve Government Radio Communications Interoperability, or otherwise;

- Agree a new strategy, to achieve interoperable communications across jurisdictions.

Recommendation 6.4: Delivery of a Public Safety Mobile Broadband capability.

Australian, state and territory governments:

- Should expedite the delivery of a Public Safety Mobile Broadband (PSMB) capability;

- As the PSMB develops, there should be a national coordinating body to oversee PSMB development and maintenance. This body would ensure ongoing efficiency of the PSMB capability and act as a coordination point to support cooperation between governments.

- This body should sit within the Australian Government, but have state and territory representation.

- Cyber Security

While the Royal Commission's Final Report carried mention of Critical Infrastructure there was no reference to cyber security and this is the case for other State and Territory Bushfire Inquiries reviewed to date.

- Visibility and Understanding of the *Ecosystem* as Critical Infrastructure

The PSMB together with Next Generation Tripe Zero will be new and transformational components of the *Ecosystem* carrying data (personal and operational) utilising the *telecommunications* networks of Mobile Network Operators (MNOs) and Mobile Virtual Network (MVNO) operators allowing Public Safety Agencies to deliver their essential services to Australian communities further reinforcing the suggestion that the *Ecosystem* falls within the category of *Systems of National Significance*.

However, it is noted that in the 194 submissions received and published by the DHACIC only two were from MNOs and none directly from Public Safety Agencies.

What cannot be ignored as Critical Infrastructure is the existing components of the *Ecosystem* i.e. State and Territory Land Mobile Radio (LMR) networks, Alerting Systems and Public Safety Agency (PSA) Communication Centres to which Triple Zero Calls are transferred after initial receipt by the Emergency Call Person.

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 greater interoperability.

The LMR networks provide high quality voice communications for both strategic and tactical communications and will provide redundancy and resilience to the *Ecosystem* when (if) *telecommunications* infrastructure fails. Therefore, it should be 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.

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.

- Evolution and Risk

The evolution of the *Ecosystem* is underway requiring national co-ordination to capture opportunities and mitigate risk to produce the considerable potential benefits from the investment involved in terms of public safety outcomes.

With these benefits and outcomes will come an increased level of risk which can be mitigated by calling upon international experience where these new components have been or are in the process of being implemented e.g. cyber security risk associated with NG 911[1] in the United States of America.

International experience has also shown that the most appropriate and effective risk mitigation strategy is one that involves from the start of consultation First Responders, coupled with technical and operational expertise drawn from Public Safety Agencies and peak industry bodies.

- Conclusion

Improving the visibility and understanding of the *Ecosystem* through consideration of the matters raised in this submission will assist in mitigation of the risks associated with its evolution and more so if these risks are recognized in the suite of associated supporting legislation being developed to protect Australia's Critical Infrastructure.

It is therefore suggested that the Royal Commission's recommendations should be recognised and incorporated through the subsequent stages of consultation by DHACIC on the Critical Infrastructure Framework to cover the total *Ecosystem* in a manner that brings into play the key stakeholders in the *Ecosystem* in anticipation of its acceptance and development as a *System of National Significance*.

[1] https://www.cisa.gov/sites/default/files/publications/NG911%20Cybersecurity%20Primer.pdf

In conclusion and in recognition of the late engagement in the consultation process associated with *Protecting Critical Infrastructure and Systems of National Significance* the CDMPS and its industry partners would seek to continue to become more fully involved in this important activity through the Sector Specific Co-Design stage to commence in early 2021.

For further information about this submission please contact:

Geoff Spring

Senior Industry Advisor

University of Melbourne

Centre for Disaster Management and Public Safety

[redacted]

Mobile: [redacted]