University of Melbourne

Centre for Disaster Management and Public Safety

Submission to the Cyber and Security Infrastructure Centre (CISC)

Comments on the Exposure Draft of the Security Legislation Amendment (Critical Infrastructure Protection) (SLACI) Bill 2022.

31 January 2022

In conjunction with Industry Partners:

Australian Radio Communications Industry Association

australian control room network association

TCCA - Australian Communications Forum

Introduction:

The University of Melbourne Centre for Disaster Management and Public Safety (CDMPS) in conjunction with its industry partners, ARCIA[1], TCCA[2] and the ACRNA[3] once again welcomes the opportunity to make this submission to the Department of Home Affairs Cyber and Security Infrastructure Centre providing comments on the Exposure Draft of the Security Legislation Amendment (Critical Infrastructure Protection) (SLACI) Bill 2022.

Purpose:

Over the past 18 months the CDMPS has made several submissions to various government entities including both the Critical Infrastructure Centre (now the Cyber and Security Infrastructure Centre - CISC) and the Parliamentary Joint Committee for Intelligence and Security (PJCIS).

These CDMPS submissions recommended that the Mission Critical (Public Safety) Communications Ecosystem (the Ecosystem) used by Australia's Public Safety Agencies be recognised in legislation as a key component of Australia's Critical Infrastructure Communications Sector.

The previous submissions provided evidence supporting the evolution of this recommendation and more recently included nomination of the Ecosystem as a *System of National Significance (SoNS*) which is now the focus of the Exposure Draft of the Security Legislation Amendment (Critical Infrastructure Protection) (SLACI) Bill 2022.

It is understood from the CISC consultation process that the intention is the Bill will be presented to Parliament during its first sitting in 2022.

Noting that the SLACI Act came into law on 22 December 2021 to better protect Australia's Critical Infrastructure from a cyber-attack and be better equipped to respond to such an attack this submission does not intend to repeat previously provided information and advice about the recommendation that the Ecosystem be recognised in legislation as a *System of National Significance.*

Instead, this submission seeks to provide an update as follows on the various components of the Ecosystem to inform policy implementation in both the strategic and operational sense as input to the industry – stakeholder consultation process currently being conducted on the Exposure Draft by CISC.

Triple Zero Service

The national Triple Zero Service is the front end of the Ecosystem provided by Telstra as the "Emergency Call Person (ECP)" for the receipt of 000 voice calls.

National media publications have identified Australia's Triple Zero service has come under stress because of the Covid – 19 and Omnicom pandemic illustrated by 000 call answering and processing times, ambulance response times and the associated issue of ramping at hospital emergency departments. This is an international issue as similar trends have been reported overseas.

[1] https://arcia.org.au/
[2] https://tcca.info/
[3] https://acrna.org/

In Victoria two government inquiries have been announced regarding delays being encountered within the 000 service and coronial inquiries are reportedly being considered as well.

Location

The accuracy of the location of an emergency incident/event continues to grow in importance as a core input to the efficient functioning of the Ecosystem. Technology evolution e.g., GPS and Advanced Mobile Location (AML) in mobile handsets is now providing the capability to identify location as part of the call receipt, processing, dispatch, and response process performed by the Ecosystem.

The availability of geospatially enhanced data in associated Spatial Data Infrastructures and Land Management Administration systems will become a major component of the Ecosystem complementing the use of voice in Public Safety Agency Communications Centres.

Public Safety Agency Communications Centres

Public Safety Agency Communications Centres perform an essential role in the efficient functioning of the Ecosystem.

Triple Zero calls are transferred by the ECP to State and Territory Governments' Public Safety Agency Communications Centres (or the Emergency Services Telecommunication Authority - (ESTA) in Victoria) where the calls are triaged using Computer Aided Dispatch (CAD) systems and police, ambulance, fire, state emergency services resources and equipment are dispatched using Land Mobile Radio (LMR) and mobile data and paging systems, and the ad hoc use of smart phones and other devices on commercial carriers wireless broadband networks, in lieu of a formal Public Safety Mobile Broadband (PSMB) capability.

New communication technologies such as machine to machine communications and artificial intelligence have the potential to significantly enhance the capabilities and capacities of these Centres. The ability to provide connectivity to support systems and services e.g. medical and automatic crash notification systems, through both government and third-party services has the potential to reduce processing and response notification times providing a significant contribution to the health and safety of all Australians including Public Safety Agency First Responders – career and volunteer.

In this context the human resourcing of the Ecosystem and the associated continuous training of these resources in the use of its evolving technologies (including First Responders as end uses) will be of high importance.

Public Safety Mobile Broadband (PSMB)

State Governments are investing in upgrading the capacity and capabilities of their LMR networks, and the communication devices used on these networks by First Responders (law enforcement, ambulance, fire, and state emergency services personal).

Globally PSMB capability is being progressively introduced to public safety communications ecosystems providing the capability to receive and process data. This PSMB capability will be further enhanced through the interfacing with rapidly evolving technologies such as the Internet of Things and Digital Twins to enable enhanced predictive decision making and responses to public safety incidents.

The Royal Commission into Australia's National Natural Disaster Management Arrangements described the lack of a PSMB as a "significant gap in the communications capability of Australia's Public Safety Agencies".

In Australia the PSMB Proof of Concept is still proceeding with outcomes not expected until late in 2022.

International Standards Development and Cyber Security

International Standards Development Organisations (SDOs) are continuing to develop standards to underpin the design and operational capacity and capability of the technologies used in the Ecosystem e.g. interfaces between LMR networks and interworking between LMR and commercial carrier 4G networks and ultimately evolution of same interfacing in 5G.

This continuing evolution of interfacing and interworking will represent an increasing risk to the security of all data being conveyed in real time across the Ecosystem and between other associated ecosystems including end-user devices increasing potential perimeter/attack surface area and therefore, an increased area for potential interception particularly after the introduction of the PSMB capability into the Ecosystem.

As these international standardised interfaces are established between different technologies within the Ecosystem the complexity of the Ecosystem itself increases and hence operational risk needs mitigation.

Energy Sector

The Communications Sector relies on the Energy Sector of Australia's Critical Infrastructure to supply a continuous supply of electricity to allow the Ecosystem to function hence the relationship with the Energy Sector and its transition to renewable sources such as battery, solar and wind power through distributed infrastructure and enhanced connections to the national and state grids becomes vitally important to the Mission Critical Ecosystem.

A stable Energy Ecosystem will support the emerging availability of "tactical dispatching" of Public Safety Agency resources through distributed Incident Control Centres as nodes on State-wide communications and energy networks with both providing enhanced network connectivity, capabilities and levels of redundancy enabling the transfer of data and hence information in real time.

Communication Towers

Communication towers are an integral component of the Ecosystem.

Private sector owned communication towers are particularly relevant to the proposed PSMB capability which currently proposes the use commercial carriers to provide the capability using towers that in the past twelve months have been progressively divested to new international owners or locally to major financial institutions.

It is assumed that this change in tower ownership is being monitored by the CISC and that the new owners of this infrastructure are involved in the CISC consultation process on the draft Legislation.

Policy Context

It could be argued that the above description of key components of the Ecosystem are "operationally" focussed rather than in the policy sense of whether the Ecosystem should be identified as a *"System of National Significance".*

The identification of the Ecosystem as a *System of National Significance* would/should bring with it the level of national interest that needs to be taken across Governments and bureaucracies to ensure that the Ecosystem is always *"fit for purpose"* through a National Risk Management Program of a type consistent with that being required of commercial and corporate entities under the Legislation contemplated by the Exposure Draft Bill 2022.

Alternatively, the adoption of the National Disaster Risk Reduction Framework[4] (DRRF) to manage government risk associated with natural disasters should be considered. The DRRF has a natural alignment with the Ecosystem and with other Critical Infrastructure Sectors which would be enhanced by recognition of the Ecosystem as a *System of National Significance*.

This alignment would allow issues that represent a risk to the Ecosystem to be pursed within government in a focussed, co-ordinated, and transparent manner to all key stakeholders and mitigate policy risk from a government perspective and corporate/operational risk from a commercial perspective.

Current examples of these issues are as follows:

- The House of Representatives Standing Committee on Infrastructure, Transport and Cities has sought advice on the status of the Government response to the Committee's 2016 Report on Smart Infrastructure[5] which recommended that *public safety communications should be recognised as critical infrastructure.*

- Progress with the implementation of the recommendations arising from the Royal Commission into Australia's Natural Disaster Arrangements were last published by the Department of Home Affairs in June 2021 i.e. seven months ago.

  The 2021/22 Bushfire Season is progressing meaning that two bushfire seasons will have come and gone since the 2019/20 Bushfire season which gave rise to the need for the Royal Commission and its recommendations to and adoption by Government.

  The absence of these reports makes impossible the monitoring of the 27 recommendations identified by the CDMPS as relevant to the Ecosystem.

- Information to key stakeholders on progress with the PSMB Proof of Concept and the associated issue of spectrum allocation for use by Public Safety Agencies consistent with the proposed business/operational model for the PSMB.

[4] https://www.homeaffairs.gov.au/emergency/files/national-disaster-risk-reduction-framework.pdf
[5] https://www.aph.gov.au/Parliamentary_Business/Committees/House/ITC/Smart_ICT/Report

- The 2021 Regional Telecommunications Review: *A step change in demand*[6], has been completed and provided to the Minister for Regionalisation, Regional Communications and Regional Education with the expectation the Report will be tabled in Parliament in early 2022.

  While the report is currently embargoed it should be expected that its recommendations will relate to the above issues and the matters raised in the Submission.

In both summary and conclusion:

If the Mission Critical Communications Ecosystem *is not identified and recognised in Legislation* as a as a *"System of National Significance"* within the Communications Sector of Australia's Critical Infrastructure then in the context of the next major natural disaster or pandemic, cyber-attack or response to a single incident that did not meet community public safety expectations the question to be answered will be *"why not"*.

For further information regarding this submission please contact:

Geoff Spring

University of Melbourne

Senior Industry Advisor

Centre for Disaster Management and Public Safety

[redacted]

[6] https://www.rtirc.gov.au/