Security of Critical Infrastructure Bill 2017

A Bill for an Act to create a framework for managing critical infrastructure, and for related purposes
incorporating matters relating to the
Home Affairs and Integrity Agencies Legislation Amendment Bill 2017

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

22 January 2018

Response to the Joint Parliamentary Committee on Security and Intelligence (JPCSI) review of the Security of Critical Infrastructure Bill 2017 – A Bill for an Act to create a framework for managing critical infrastructure, and related purposes.

1.0 Introduction

The University of Melbourne's Centre for Disaster Management and Public Safety (CDMPS)[1] welcomes the opportunity to provide a submission responding to the Joint Parliamentary Committee on Security and Intelligence (JPCSI) review of the Security of Critical Infrastructure Bill 2017 – A Bill for an Act to create a framework for managing critical infrastructure, and related purposes.

This submission is consistent with the CDMP's strategic intent to support multi-disciplinary collaboration between researchers, government, industry, public safety and national security agencies and the community in delivering enhanced decision making capabilities resulting in increased community safety resilience and public safety outcomes.

This submission also continues to build upon and references previous CDMPS submissions responding to a range of Australian Government and Federal Government Department Discussion Papers related to individual components of the *mission critical public safety communications ecosystem*. In particular this submission refers to the following two previous CDMPS submissions:

(a) The Critical Infrastructure Centre's Discussion Paper on "Strengthening The National Security of Australia's Critical Infrastructure" – March 2017;

(b) 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 all Australian Governments and Territories – January 2018.

Copies of these CDMPS submissions are attached to this response.

2.0 Purpose

The purpose of this response to the JPCSI is to continue to identify:

(a) The need for the Australian Government to recognise Australia's mission critical public safety communications ecosystem as Critical Infrastructure;

(b) The Australian Government and Federal Government Departments are *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

---

[1] http://research.unimelb.edu.au/cdmps

bureaucratic decision makers, Public Safety Agencies (PSAS), First Responders, national security agencies and all Australians.

3.0 Opportunities

CDMPS research has identified a number of opportunities for the Australian Government to consider in relation to Australia's evolving mission critical public safety communications ecosystem as follows:

1. The opportunity for the Australia Government to consider the recommendation of the House of Representatives Standing Committee on Infrastructure, Transportation and Cities in 2016[2] that *mission critical public safety communications be considered as critical infrastructure.*

2. The opportunity to provide a safe and secure working environment for the First Responders in Australia's PSAs and national security agencies as they attempt to keep all Australians safe from harm by sharing intelligence generated through use of the PSMB capability specifically and the mission critical public safety communications ecosystem more generally.

3. 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 in encouraging private sector involvement and investment in the public safety market and the evolution of the mission critical public safety communications ecosystem.

4. The opportunity to formally constitute a national co-ordination body to provide collaborative leadership, policy direction and strategic oversight to the evolution of the mission critical public safety communications ecosystem.

5. 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.

6. The opportunity to establish a trusted relationship between the public safety community, governments, industry and academia to address the impact of technological and associated organisational and cultural change in terms of public expectation and confidence.

7. The opportunity to establish a research capability leveraging international experience to support Australia's PSAs and national security agencies in using public safety specific technologies to facilitate innovation in enhanced decision making, personal protection, productivity, and public safety outcomes.

The suggested opportunities for the Australian Government in relation to Australia's evolving mission critical public safety communications ecosystem align with the Framework created by the Security of Critical Infrastructure Bill 2017 to manage risks to national security relating to critical infrastructure.

[2] https://www.aph.gov.au/Parliamentary_Business/Committees/House/ITC/Smart_ICT/Report

4.0 Related Government Legislation, inquiries and announcements

CDMPS research has also identified previous and current Australian Government and Federal Department legislation, inquiries, decisions and announcements linked to the mission critical public safety communications ecosystem and hence to the Security of Critical Infrastructure Bill 2017 as follows:

- Next Generation Triple Zero Tender.
- House of Representatives Standing Committee on Infrastructure, Transportation and Cities 2016 Inquiry on the role of smart ICT in the design and planning of infrastructure.
- The Australian Government's Telecommunications Sector Security Reform (TSSR) Legislation.
- The Australian Competition and Consumer Commission Domestic Mobile Roaming Declaration Inquiry.
- The Australian Competition and Consumer Commission Australian Communications Study.

CDMPS research has also identified the following related current reviews, inquiries, policy initiatives decisions:

- The Joint Parliamentary Committee for Law Enforcement (JPCLE) initiated an inquiry into the impact of new and emerging information and communications technology.

- The Australian Government's Home Affairs and Integrity Agencies Legislation Amendment Bill 2017.

- The advice to be provided to the February meeting of the Council of Australian Governments (COAG) on the outcome from the Request for Information (RFI) relating to a national Public Safety Mobile Broadband (PSMB) capability.

In preparing this submission matters related to the the Australian Government's Home Affairs and Integrity Agencies Legislation Amendment Bill 2017 have been identified around the use of the mission critical public safety communications ecosystem and in particular the PSMB capability by national security agencies.

It is noted that the Home Affairs and Integrity Agencies Legislation Amendment Bill 2017 is about machinery of government changes required to support the functioning of the Home Affairs and Attorney Generals' Departments.

Rather than making a separate submission to the JPCLE Home Affairs and Integrity Agencies Legislation Amendment Bill 2017 which would simply duplicate matters addressed in this submission commentary about Department of Home Affairs matters issues has been included in this submission (Refer Section 4.1).

4.0 Specific Issues related to the Security of Critical Infrastructure Bill 2017

In January 2017 the Australian Government launched the Critical Infrastructure Centre[3] which subsequently identified Australia's most critical infrastructure as being electricity, water, ports and c*ommunications.*

[3] https://www.ag.gov.au/NationalSecurity/InfrastructureResilience/Pages/default.aspx

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

4.1 Public Safety Mobile Broadband (PSMB)

The Australian Government accepted the advice provided by the Productivity Commission that the least-cost option to provide Australia's PSAs with a PSMB capability is to use a commercial carrier.

Cyber security is a major risk for the mission critical public safety communications ecosystem and the PSAs that rely on the ecosystem. This risk will further increase with the proposed new PSMB network because of the nature of the data carried by the network and the use to which it will be put by PSAs.

In addition to PSAs the Federal Government in previous iterations of PSMB capability required provision for agencies such as the Australian Federal Police and the predecessors of Australian Border Force. It is assumed that this requirement remains in place and that these agencies may require their own specific service delivery model and level of cyber security associated with their use of the ecosystem generally and specifically the PSMB capability.

The Security of Critical Infrastructure Bill 2017 needs to recognise the link between the mission critical public safety communications ecosystem and the proposed PSMB capability to the national security agencies within the new Home Affairs Department and the Attorney Generals' Department.

4.2 Telecommunications Sector Security Reform (TSSR) Legislation

The Security of Critical Infrastructure Bill 2017 transfers *telecommunications* to the TSSR Legislation due to become operational by September 2018. The TSSR Legislation introduces obligations on carriers and carriage service providers to *do their best* to protect networks and facilities from unauthorised access and interference.

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; and public confidence in and expectations of Australia's PSAs and national security agencies. It is anticipated that 'best effort' provisions fall short of this standard of environment.

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

4.3 PSMB Mobile Roaming

The ACCC's inquiry into the need for a domestic mobile roaming service expressed a preliminary view that the supply of a mobile roaming service is technically feasible noting domestic and international commercial roaming arrangements that have been, or currently are, in place in Australia.

Public Safety Communications Europe [4](PSCE) has identified the need for the review of European Union (EU) policy and regulation regarding mobile telecommunications. This review would address 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.

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.

Confirmation by Australia's PSAs and national security agencies of a mobile roaming requirement will need to be included in the cyber security environment for the mission critical public safety communications ecosystem and should be addressed through the Security of Critical Infrastructure Bill 2017 and the TSSR.

4.4 Future Proofing

Cyber security for the evolving mission critical public safety communications ecosystem needs to be robust enough take into account the impact of technology developments such as Collaborative Intelligent Transport Systems (C-ITS)[5] and the Internet of (Public Safety) Things. This robustness is essential because by the time the PSMB capability is delivered and uniformly in use nationally many of the technology concepts mentioned as future developments will be in place.

5.0 Conclusion

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 utilise the mission critical public safety communications ecosystem in managing risks to national security and provide a base for determining the level of cyber security protection required for the evolving ecosystem and its use by Australian PSAs and national security agencies.

---

[4] www.psc-europe.eu
[5] https://imovecrc.com/

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 incorporating commercial partnerships and PSMB capability.

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