DATA TO DECISIONS CRC
UNLOCKING THE VALUE OF AUSTRALIA'S DATA

Base 64
64 North Terrace, Kent Town
Adelaide SA 5067

info@d2dcrc.com.au

www.d2dcrc.com.au
ABN 45 168 769 677

January 12, 2018

Mr Craig Kelly MP
Chair, Joint Committee on Law Enforcement
Parliament House
Canberra ACT 2600

Dear Chair,

Re: Inquiry into the impact of new and emerging information and communications technology

Please find below a submission to the inquiry into the Impact of New and Emerging Information and Communications Technology (ICT) by the Parliamentary Joint Committee on Law Enforcement. This submission is made by the Data to Decisions Cooperative Research Centre (D2D CRC). We have specifically focused on the items in bold in the terms of reference below:

> *Pursuant to subsection 7(1) of the Parliamentary Joint Committee on Law Enforcement Act 2010, the committee will examine the impact of new and emerging information and communications technology (ICT) with particular reference to:*
>
> ***a. challenges facing Australian law enforcement agencies arising from new and emerging ICT;***
>
> *b. the ICT capabilities of Australian law enforcement agencies;*
>
> ***c. engagement by Australian law enforcement agencies in our region;***
>
> *d. the role and use of the dark web;*
>
> *e. the role and use of encryption, encryption services and encrypted devices; and*
>
> ***f. other relevant matters.***

We appreciate the committee's time and consideration on this important topic and are happy to participate further at the committee's request.

Please contact me should you wish to discuss this submission in further detail.

Yours sincerely,

Dr Sanjay Mazumdar
Chief Executive Officer

DATA TO DECISIONS CRC
UNLOCKING THE VALUE OF AUSTRALIA'S DATA

Base 64
64 North Terrace, Kent Town
Adelaide SA 5067

info@d2dcrc.com.au
Phone +61 8 8302 8978
www.d2dcrc.com.au
ABN 45 168 769 677

Introduction

Established with a grant of $25 million in July 2014, the Data to Decisions CRC (D2D CRC) is part of the Australian Federal Government's Cooperative Research Centres Program. The D2D CRC brings together researchers and industry to tackle the big data challenges faced by the agencies of Australia's National Security Community - Law Enforcement Agencies (LEAs), Australian Intelligence Community (AIC) and Defence. Specifically, the D2D CRC is collaborating with members of the National Security Community to develop capabilities (tools, techniques, know-how and people) to support the agencies to employ advanced big data analytics for their respective national security responsibilities.

The Threat Landscape

The threat landscape for national security and law enforcement agencies continues to evolve at an unprecedented rate.

As noted in the AFP's *Strategy for Future Capability*[1] released in 2017, threat actors of all persuasions are early adopters of rapidly emerging social media and other instantaneous communication technologies (some of which are heavily encrypted). Organised crime groups utilise these emergent technologies as ways of coordinating their activities, while counter-terrorism actors relay heavily on fast paced multi-media technologies to recruit and spread propaganda.

Traditional capability development in the national security and law enforcement community has often been done within single agency walls and stove piped from other agencies who share like problems and like data sets. Moreover, the pace of development or insertion of new capabilities in national security agencies is traditionally slow and complex.

The mismatch between the rapid update of new technologies by threat actors and the less agile capability development activities in agencies will only increase unless new approaches to fostering capability development within the AIC and LEAs are adopted.

The need for better capability development approaches applies to a broad range of security domains, including border security, financial intelligence, defence, counter terrorism and cyber security. Cooperative relationships must be forged between national security agencies, academia and industry partners to foster a culture of capability 'co-creation' where like technical needs are identified and addressed openly and in a collaborative manner.

---

[1] AFP, *Policing for a Safer Australia: strategy for future capability:* [1] AFP, https://www.afp.gov.au/sites/default/files/PDF/strategy-for-future-capability.pdf

DATA TO DECISIONS CRC
UNLOCKING THE VALUE OF AUSTRALIA'S DATA

Base 64
64 North Terrace, Kent Town
Adelaide SA 5067

info@d2dcrc.com.au
Phone +61 8 8302 8978
www.d2dcrc.com.au
ABN 45 168 769 677

Capability Development Needs

As outlined in the AFP's *Strategy for Future Capability* and the 2017 *Independent Intelligence Review*[2], information sharing, advanced analytics, new legal and policy regimes and collaborative approaches to address common capability needs across the national security community will enable threats to be identified and mitigated much quicker.

As identified in the D2D CRC's research and development program, AFP's *Strategy for Future Capability* and 2017 *Independent Intelligence Review,* these common capability needs are in areas such as:

- advanced data analytics;
- big data architectures, platforms and technologies;
- big data collection, processing, analysis and reporting;
- augmented and mixed reality technologies for interacting with and understanding data;
- information sharing and entity linkage;
- understanding contemporary societal and psychological drivers and motivations for crime including extremism;
- law and policy development and implementation; and
- big data workforce development.

In some instances, the lack of community-wide visibility of these common capability needs has resulted in overlapping development projects, parallel approaches to market or missed opportunities to integrate capabilities that would achieve a better outcome for the national security and law enforcement community. Moreover, the varying levels of technical maturity and sophistication across the agencies, different capability development frameworks and legislative or policy constraints have impacted on the ability to transfer technologies and capabilities across the community. These issues have been recognised by the national security agencies and they are attempting to address them through their active support of the D2D CRC and the establishment of coordination committees such as the National Security Science and Technology Inter-Departmental Committee. However, more needs to be done given the rapidly evolving threat environment and pace of change of technology.

A Proposed Solution

The D2D CRC is currently working with several agencies and research providers to harmonise the national security needs and develop capabilities in some of the areas mentioned above. In doing so, it has become evident that there will be a need beyond the end of the D2D CRC (30 June 2019) to continue and expand this role. Specifically, the CRC's current activities have highlighted the need for:

- effective sharing and coordination of the national security community's data analytics capabilities;

---

[2] Commonwealth of Australia, Department of the Prime Minister and Cabinet, *2017 Independent Intelligence Review.*

DATA TO DECISIONS CRC
UNLOCKING THE VALUE OF AUSTRALIA'S DATA

Base 64
64 North Terrace, Kent Town
Adelaide SA 5067

info@d2dcrc.com.au
Phone +61 8 8302 8978
www.d2dcrc.com.au
ABN 45 168 769 677

- the development of common capabilities across the community;
- a coordinated approach to legislative and policy changes to support agencies' functions; and
- a coordinated approach to assess and address current and emerging technology and workforce gaps.

As a result, the D2D CRC has recently developed a concept proposal for a new CRC, the **INdata CRC**. This new CRC would leverage the infrastructure, expertise and collaborative relationships established in the D2D CRC to address the common big data and information sharing needs across national security and law enforcement agencies.

INdata CRC would focus on the integration of technical capabilities across the Commonwealth, identifying areas for collaboration, convergence or deconfliction, and ultimately leading to improved data analytic capabilities to support decision makers, as well as more efficient and effective utilisation of data already held by agencies. INdata CRC would also be well positioned to exploit opportunities to transfer technology to other sectors as appropriate. To achieve this, INdata CRC would work closely with agencies' business managers and capability development groups, industry, the Australian Cyber Security Growth Network (ACSGN), as well as other R&D partners, both national (Defence Science and Technology Group and Data61) and international.

In summary, INdata CRC would focus on:

- **developing innovative solutions** to common capability needs;
- **standardising** architectures, platforms and practices;
- providing independent technical **advice**;
- **forecasting** relevant technological advancements and trends;
- researching and developing **law and policy frameworks**;
- **educating and training** the data analytics workforce; and
- **researching** new capabilities for law enforcement and intelligence.

In conclusion, the challenges being faced by law enforcement agencies and the broader national security community in a highly digitised and deeply connected threat environment is driven by bad actors who leverage state-of-the-art, commercially available technologies to pursue their goals. To stay ahead of these threat actors, national security agencies must move past seeing capability development and data holdings as 'proprietary'. Instead they must be open to agile and collaborative capability development approaches where partner agencies with common needs collaborate with a network of trusted national and international public and private partners. It is our belief that the proposed INdata CRC would help to address this need.