PROSPECTUS

INdata
CRC BUILDING A SAFE AND SECURE NATION

VISION AND MISSION

INDATA CRC WILL PARTNER WITH AUSTRALIA'S NATIONAL SECURITY COMMUNITY TO DEVELOP TOOLS TO ANALYSE AND UNDERSTAND BIG DATA, WITH THE GOAL OF BUILDING A SAFER AND MORE SECURE NATION

The ground-breaking tools developed by INdata CRC will empower national security agencies to analyse, understand and share complex information, much of which they struggle to uncover. This will provide them with a stronger capability to gather intelligence, investigate crime, prosecute criminals, manage security risks and protect the nation's borders.

The tools developed by the CRC will also be readily transferable to other sectors to significantly improve their data analytics capabilities.

CONTENTS

THE NEED

THE THREAT LANDSCAPE FOR NATIONAL SECURITY AGENCIES CONTINUES TO EVOLVE AT AN UNPRECEDENTED RATE

Terrorist and criminal activities are growing globally and becoming increasingly sophisticated. The use of new technologies by these groups offers them the ability to plan and coordinate attacks and crimes with impunity. The sheer volume of data and complexity driven by use of diverse software applications means much of the activity remains hidden. The need to develop and apply advanced data analytics capabilities and tools has never been more acute. The proposed INdata CRC will focus on developing these in partnership with national security agencies to generate timely and accurate intelligence to counter such threats.

The need applies to a broad range of national security domains, across border security, financial intelligence, defence, counter terrorism and cyber security, examples of challenges include:

- **Border security** – the challenge is to understand the risks to Australia's borders from passenger and cargo movements.
- **Financial intelligence** – the challenge is to understand the money trail from criminal activities such as counter-terrorism financing or money-laundering.
- **Defence** – the challenge is to gain improved situational awareness for military operations through integrated analysis of multiple sources of intelligence.

- **Counter-terrorism** – the challenge is timely identification of threat actors to prevent catastrophic events from occurring.
- **Cyber security** – the challenge is to get ahead of hackers by applying intelligence capability to predict attacks.

The big data challenge is relevant to all the domains, with investigators and analysts spending much of their time collecting and formatting data rather than undertaking deeper analysis. The application of advanced analytics to automate lower value work allows their skills to be applied to creating high value intelligence leading to better informed decision making.

New capabilities and tools must be developed to support the national security agencies to achieve their mission of creating a safer and more secure nation. The INdata CRC will focus on addressing this rapidly evolving community-wide capability needs, data sharing needs and the associated legal and policy challenges – these are the subjects of key recommendations in the *2017 Independent Intelligence Review*[1]. To support the development of innovative solutions to these capability needs, the INdata CRC will facilitate ground breaking research in areas such as:

- cognitive computing and machine learning;
- graph computing and analytics;
- multimedia analytics and understanding;
- knowledge discovery and dissemination;
- narrative visualisation using augmented reality; and
- enabling legal and policy frameworks.

TO SUMMARISE, THE GOAL OF THE INDATA CRC WILL BE:

BUILDING BIG DATA CAPABILITY TO CREATE A SAFER AND MORE SECURE NATION

[1] *2017 Independent Intelligence Review* – https://pmc.gov.au/sites/default/files/publications/2017-Independent-Intelligence-Review.pdf.

“

THE NEED TO DEVELOP AND APPLY ADVANCED DATA ANALYTICS CAPABILITIES AND TOOLS HAS NEVER BEEN MORE ACUTE

SCOPE OF INDATA CRC ACTIVITIES

The proposed programs for the INdata CRC have been formed through continuing consultation with prospective end-user[2] participants, including both national security agencies and relevant industry end-users. They are summarised in the following program architecture:

BORDER MANAGEMENT AND SECURITY INVESTIGATIONS	FINANCIAL INTELLIGENCE	MULTI-INT ANALYTICS	COUNTER TERRORISM AND LAW ENFORCEMENT INVESTIGATIONS	CYBER THREAT INTELLIGENCE
ENABLING LEGAL AND POLICY FRAMEWORKS				
WORKFORCE DEVELOPMENT				

[2] End-users refers to national security agencies and industry partners who are the end beneficiaries of the outputs of the CRC, i.e. the ultimate customer of the CRC.

SCOPE OF INDATA CRC ACTIVITIES

PROGRAM 1: BORDER MOVEMENT AND SECURITY INVESTIGATIONS

Managing the movement of people and goods across Australia's border is critical for maintaining national security. The large volume of legitimate trade and travel and the low frequency of threats makes risk detection a challenging problem, one that is only becoming more difficult as the methods used to bypass border protections become increasingly sophisticated. At the same time, detection and prevention of threats to Australian citizens must be balanced against the need to facilitate efficient movement of passengers and cargo.

These challenges require an advanced, automated approach to risk assessment which is not currently available or being used optimally. Analysts and border protection staff need the ability to quickly understand the risk associated with a person or piece of cargo. This information can be used to target cargo for inspection, optimising the use of limited human resources, and flag risky travellers for assessment, thereby reducing the threat to Australia.

The risk assessments performed for border movements can benefit significantly from "graph" information, i.e. a network of entities and their relationships, constructed from many data sources (e.g. visa, customs, law enforcement, open source data). This graph data can be analysed to associate border movements with risk entities, either directly or through multiple degrees of separation, and to identify risky entities based on their patterns of behaviour over time. INdata CRC will develop new graph analytics to significantly improve the efficiency and effectiveness of these assessments.

Specific examples include:

- determining that a traveller is closely related to someone involved in a previous cargo seizure (cross-domain entity linking);
- determining that a package from a high-risk country is being delivered to the neighbour of a known drug dealer (geo-spatial analysis);
- discovering a group of people connected in a similar way to a known organised crime group (graph pattern matching); and
- detecting a male repeatedly entering the country with different females and leaving alone, potentially indicating sex trafficking (pattern of life analysis).

PROGRAM 2: FINANCIAL INTELLIGENCE

In May 2017, the World Economic Forum held a workshop on the main challenges in financial crime management, a general function covering anti-money laundering (AML), combating the financing of terrorism (CTF) and sanctions. The goal of effective financial crime management (FCM) is to identify "bad actors" (criminals, terrorists or rogue states) in the financial system, enable their prosecution and conviction and support asset forfeiture to disrupt criminal enterprises. International standards require regulators and financial institutions to follow a risk-based approach when they design and implement their financial crime measures. The report highlighted that FCM can benefit significantly from the application of advanced analytics. Three key areas are:

Risk profiling and monitoring

Know Your Customer, profiling and transaction monitoring

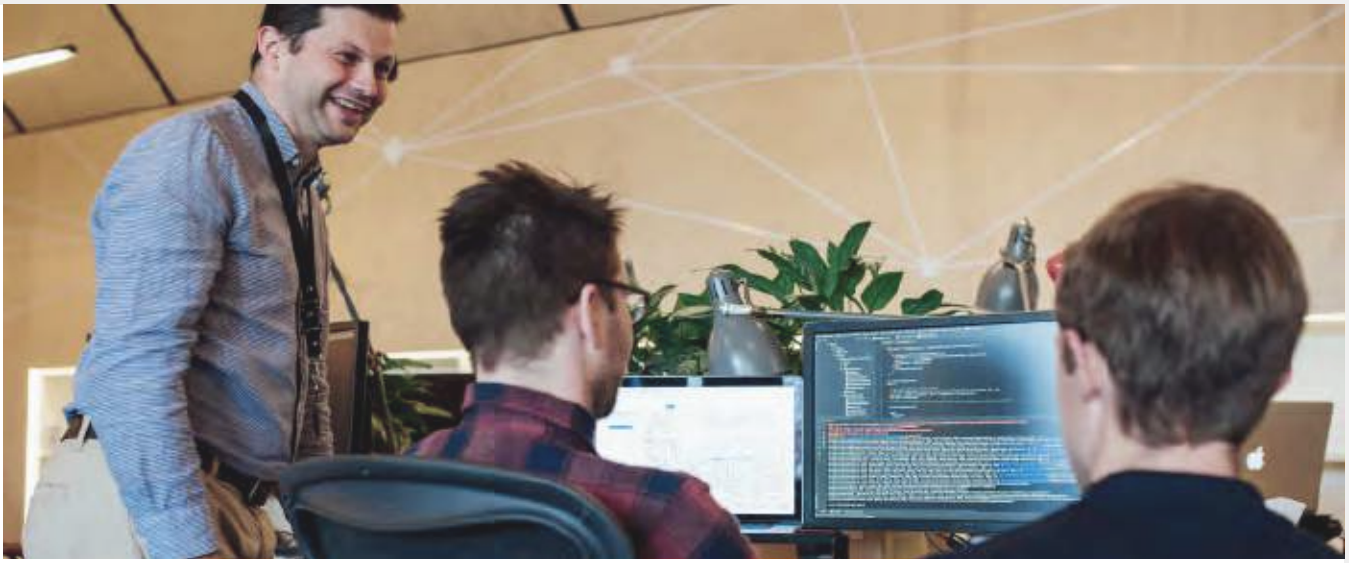
Institutions regulated by AML/CFT are required to implement Customer Due Diligence (CDD) measures. This includes Know Your Customer (KYC) processes (customer identification and verification), risk profiling of the customer and monitoring of the customer's transactions to identify unusual and suspicious transactions. Where a customer poses a higher risk, more extensive CDD must be undertaken. Current approaches to KYC/CDD are generally informed by very basic risk-scoring models and investigations of transactions often involve inefficient data practices. The proposed INdata CRC will develop graph analytics and machine learning techniques to automate these processes, resulting in significant productivity improvements and greater

SCOPE OF INDATA CRC ACTIVITIES

accuracy in risk scores. Moreover, such techniques combined with advanced entity matching can support a single view of a customer and their linked entities across the financial ecosystem, providing a more efficient application of that profile in transactional analysis.

Country risk

FCM measures must factor in country crime risk when institutions deal with international clients and transactions. Institutions lack access to reliable, real time country data to inform jurisdictional crime profiles. The application of unsophisticated country risk profiles facilitated the termination of cross-border correspondent banking relationships, causing a crisis that the G20 and Financial Stability Board is attempting to address. INdata CRC will develop and integrate graph analytics and machine learning to greatly increase the accuracy and efficiency of country risk analysis and facilitate the application of the analysis to customer behaviour and transactional patterns.



Account and activity monitoring

Current FCM controls are primarily rule-based and heuristic and these techniques do not scale well with big data sets. As a result, it is difficult and expensive for financial institutions to stay ahead of the bad actors. More advanced and adaptive approaches to transaction monitoring and investigation would allow banks to identify criminal behaviour and actors. This FCM measure can benefit particularly from the application of graph analytics and machine learning to track flows of funds across time, detect anomalous patterns in vast volumes of data and automatically bring bad actors to the surface of the data.

Intermediary Financial Intelligence Units

Currently financial crime monitoring is undertaken individually by institutions, with limited sharing of findings or best practices and limited feedback on reports that were filed with the Financial Intelligence Unit (FIU). This siloed approach undermines FCM as well as law enforcement.

Technology now enables the construction of secure intermediary financial units in industries, allowing banks to share and link crime data across banking systems and collaborate closer with the AML/CFT regulator and law enforcement. Some moves to a fusion group-type model have already been made, but still richer "graph" information about potential bad actors and their transaction networks could be shared. Investment in big data analytics on this network of transactions could benefit the entire system, resulting in decreased costs to the system and improved financial crime control outcomes.

SCOPE OF INDATA CRC ACTIVITIES

PROGRAM 3: MULTI-INT ANALYTICS

The 2016 Defence White Paper and the 2017 Independent Intelligence Review emphasised the importance of strengthening the nation's intelligence, surveillance and reconnaissance (ISR) capabilities to ensure that the defence forces have the best battlespace awareness to successfully plan and conduct future operations. Historically, this has involved the siloed analysis of traditional defence data sources such as signals intelligence (SIGINT), measurement and signature intelligence (MASINT) and geospatial intelligence (GEOINT).

However, in today's big data world there is important operational intelligence increasingly found in non-traditional data sources such as open source data (OSINT). Using advanced analysis techniques and search capabilities. INdata CRC will draw upon these various data sources to reveal the information that is required to answer questions posed by mission planners, operators and intelligence analysts.

The need for timely collection, analysis and preparation of Intelligence Mission Data is increasingly required by Defence to provide an understanding of foreign threat capabilities that is critical to the development and deployment of current & future Australian military platforms.

INdata CRC will develop new interactive knowledge extraction techniques and predictive analytics that will allow defence analyst and operators to better address their information needs at the operational and strategic level.

Specific examples include:

- systems to enable timely search, preparation and analysis of data to deliver the intelligence mission data (IMD) that modern weapon systems and platforms need to work effectively;
- real-time, predictive, geo-dynamic analytics extracting, combining and presenting signals from multiple information sources (e.g. SIGINT and OSINT) – affording analysts more complete situational awareness and providing indicators of future actions; and
- automatically compiling Wikipedia-style knowledge bases on organisations and actors to lighten the cognitive load on intelligence analysts. For example, a geospatial intelligence analyst can be presented with a summary of all known facts that relate to a sea-borne vessel of interest.

PROGRAM 4: COUNTER TERRORISM AND LAW ENFORCEMENT INVESTIGATIONS

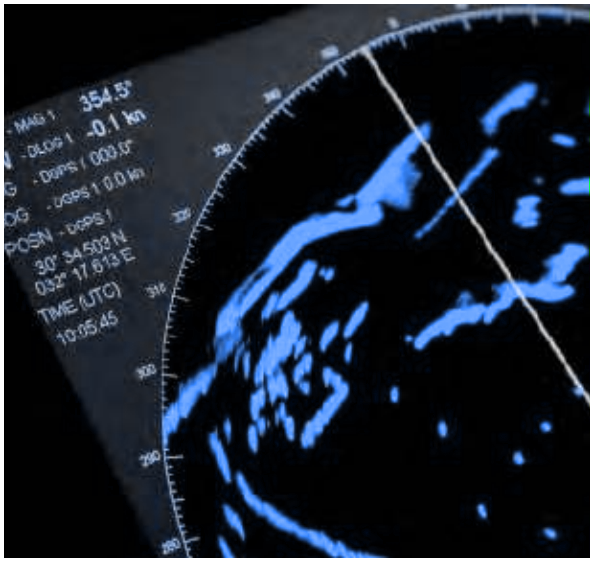
Advanced Investigation Management

Effective law enforcement relies heavily on breaking down information barriers to produce relevant insights; it is imperative that they fully leverage advances in analytics, real-time collaboration and data-driven storytelling. INdata CRC will extend the state of the art by researching and delivering data analytics and cognitive computing capability that can support case management, so that investigators and analysts can dramatically improve and automate processes to extract information and develop domain relevant intelligence through creation of entity profiles, charts, timelines and rich data-driven narratives through visualisation technologies.

INdata CRC will develop techniques that will enable current practices to be transformed through the new mantra of connectivity, curation and collaboration.

The overall goal is to provide:

- cognitive computing techniques and smart interfaces so that users can cope with the 'information overload' experienced in many investigations;
- visualisation and data-driven storytelling capabilities that allow rapid and effective understanding of the key events in a case; and
- intelligence directly to investigators – using smart tools powered by cognitive computing techniques, investigators can ask the questions they need answered. For example, "do any of my persons of interest (POIs) have links to people that have travelled to Thailand?"



SCOPE OF INDATA CRC ACTIVITIES

Risk profiling for counter-terrorism (CT), fraud and serious and organised crime

Within an integrated information environment, it is possible to begin thinking of law enforcement agencies holdings as a data graph – people and the events that bind them, connected together into a network graph. This representation of data, from a single investigation or more importantly, from the enterprise will enable INdata CRC to develop tools to support new ways of policing:

- Detection of convergence – where there are two investigations touching on the same subject matter, there is potential to develop a more complete picture of the people of interest and their activities that can lead to new charges or proactively preventing crimes (e.g. victims of domestic violence).
- Intelligence-led policing – patterns of behaviour (travel, communication etc) that were evident in one case have been subsequently identified in other data holdings and therefore warrant further investigation.
- Risk assessed POIs – CT persons of interest can be more completely risk-assessed by bringing together open source data and agency data holdings.
- Insider threats – security vetting techniques can be enhanced through continual monitoring and risk assessment across a broad range of data holdings to support the detection of insider threats.

PROGRAM 5: CYBER THREAT INTELLIGENCE

Cyber attacks are a growing security threat for Australia and other nations. Individuals, companies and government are increasingly the targets of bad actors looking to undertake identity theft, cyber-enabled economic espionage, politically motivated cyber-attacks and other malicious activity. Current cyber security approaches involve better detecting, deterring and responding to threats and risks to critical infrastructure, networks and intellectual property. Cyber threat intelligence involves devising preventive measures in advance of an attack by analysing various sources of intelligence, such as open source intelligence (OSINT), social media intelligence (SOCMINT), human Intelligence (HUMINT) or intelligence from the deep and dark web. Earlier detection of cyber attacks and alerting will allow a reduction in their impact on Australian organisations. The need to get 'ahead of the hackers' has been recognised in the Australian Cyber Security Growth Network's Cyber Security Sector Competitiveness Plan[3]. In fact, Knowledge Priority 1 in the plan is "Emerging prevention, detection and response technologies". INdata CRC will develop new techniques to detect events and themes in a broad range of data sources to predict cyber threats.

Specific examples include:

- Cyber event prediction – new automated methods will be developed to provide early indication of cyber attacks by analysing a broad range of data sources such as Twitter, Reddit, security research blogs and hacker forums.
- Strategic threat reporting – new techniques will be developed to identify strategic level threats (e.g. nation state or an industry sector) to determine who is targeting whom and why are they being targeted.
- Detection and characterisation of cyber-enabled influence campaigns – a tool will be developed to detect and characterise modern online influence campaigns by extracting themes (text, images, videos, etc) from known propaganda sites and sympathisers and automatically trace their distribution path via online media.

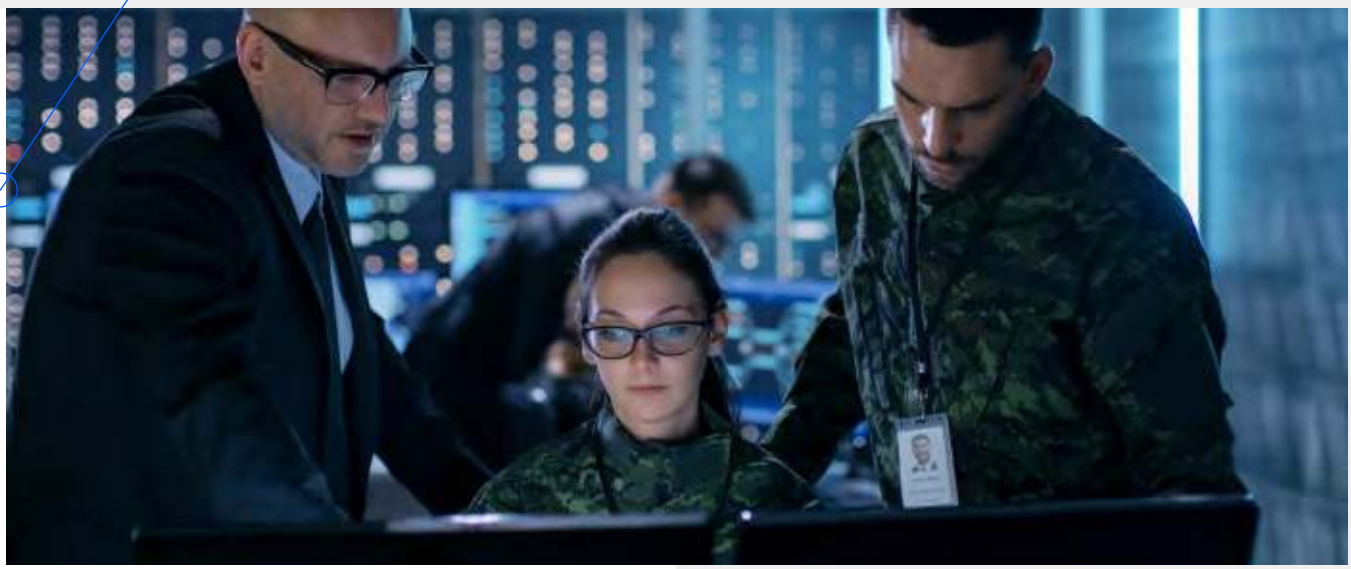
[3] https://www.acsgn.com/cyber-security-sector-competitiveness-plan/

SCOPE OF INDATA CRC ACTIVITIES

PROGRAM 6: ENABLING LEGAL AND POLICY FRAMEWORKS

One of the key recommendations in the 2017 Independent Intelligence Review is that there is a need to develop a legislative framework for Australia's intelligence community which is clear, coherent and contains consistent protections for Australians. This need applies to the broader national security community as well, including the law enforcement agencies and defence. It is therefore proposed that INdata CRC will help support this capability need and the other R&D programs by:

- defining enabling policy and regulatory frameworks to support the development and implementation of the aforementioned systems;
- establishing principles to guide R&D teams, policy makers and users in in the design, regulation, implementation, governance and oversight of these systems; and
- providing independent advice to the national security community on relevant legal and policy frameworks.



PROGRAM 7: WORKFORCE DEVELOPMENT PROGRAM

Underpinning the five programs, the INdata CRC will provide critical workforce development opportunities for Australian industry (including the national security community) by strengthening the links between industry, academia and the R&D sector. This will include building the future data science workforce through education programs and up-skilling the current data science workforce through development programs.

There will also be a focus on building the data analytics capability of industry, in general, through organisational design, research and consultancy. Moreover, there is a recognition that in the rapidly expanding digital economy, the growth of small-to-medium enterprises (SMEs), start-ups and sectors that are traditionally not digitally-driven can be accelerated through access to scarce data science expertise. A company and sector development program will be established to support this goal.

Specifically, the INdata CRC's workforce development program will focus on the following activities:

Future workforce

- sponsoring PhD, honours and masters students to work on industry relevant projects;
- creating a network and development programs for a career-ready future workforce; and
- supporting STEM, internship and gender diversity programs.

Current workforce

- development programs, including training courses, master classes and seminars for practicing data scientists and data analysts;
- organisational development research and consultancy to help agencies transition to data driven organisations; and
- deployment of the Data Science Competency Framework to support workforce development initiatives.

Company and sector development

- accelerator and mentoring programs for start-ups and SMEs; and
- translation of capabilities and know-how to other sectors, e.g. agriculture, advanced manufacturing through Industry Growth Centres, other CRCs and contract R&D.


“
INDATA CRC WILL DELIVER INNOVATIVE SOLUTIONS TO CRITICAL NATIONAL SECURITY CAPABILITY NEEDS

WHAT WILL INDATA CRC DELIVER?

BY FOCUSING ON THE PROGRAM OF ACTIVITIES DESCRIBED ABOVE, THE INDATA CRC WILL:

- deliver **innovative solutions** to critical national security capability needs;
- undertake **ground-breaking research** into new capabilities for the national security community;
- **harmonise** architectures, platforms and practices across the national security community;
- provide **independent technical advice** to support technology forecasting and capability development;
- support the development of **enabling legal and policy frameworks**;
- address critical current and future data science **workforce needs** through an education, training and consultancy program; and
- help **accelerate the growth** of SMEs, start-ups and other sectors with a data science need.

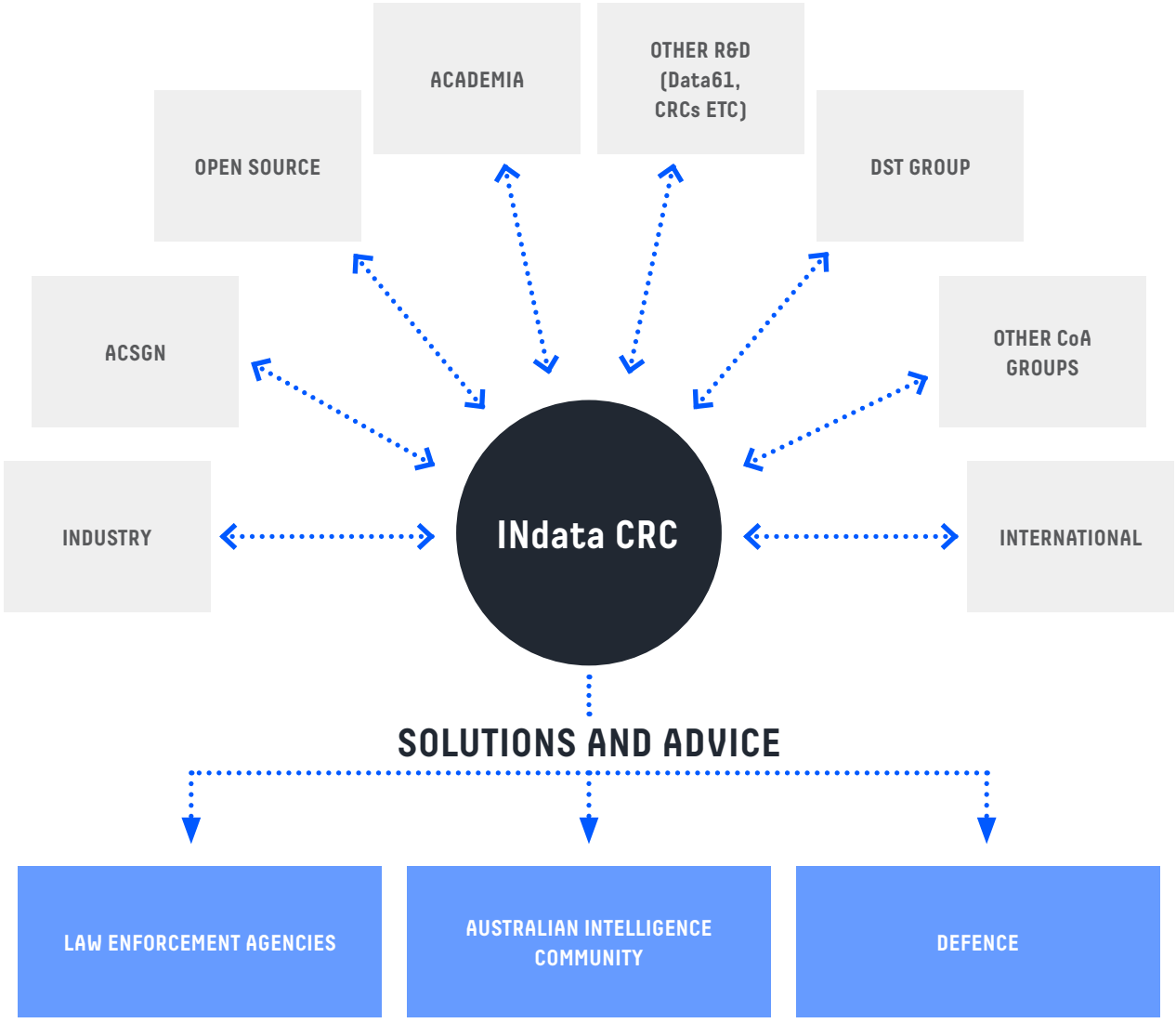
HOW WILL INDATA CRC OPERATE?

It is proposed that the INdata CRC would operate as a 'hub and spoke' model with the following elements:

- a headquarters in Adelaide leveraging the existing D2D CRC infrastructure where the main R&D and innovation activities are undertaken (hub);
- an innovation node in Canberra to enable experimentation, testing and training before deployment into agency environments (the 'spokes'). This co-development space will give agencies access to INdata CRC's capabilities and enable agency staff to work with data science, machine learning and software engineering experts; and
- additional 'spokes' comprising staff in agency capability teams to further tailor solutions to specific agency needs and ultimately operationalise them.

The 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 (e.g. Lab41, IARPA).

A VISUAL DEPICTION OF THE INDATA CRC IS SHOWN BELOW:



HOW WILL INDATA CRC OPERATE?

INTELLECTUAL PROPERTY (IP) PRINCIPLES

Each project in the INdata CRC will be governed by agreements, which among other things, will define how IP will be managed for that project including ownership, access, licensing and utilisation. The general principles that will be adopted by the INdata CRC are:

- IP resulting from a project will be legally and beneficially owned by INdata CRC;
- participants who actively engage and participate within projects will have their contributions recognised through increased rights to project IP;
- ownership of background IP stays with the party that contributes it;
- utilisation pathways for IP will be determined on the basis of balancing (1) end-user needs and (2) what will maximise the value generated from the IP for the community as a whole; and
- the most appropriate form of IP protection will be determined on a case-by-case basis balancing (1) end-user needs and (2) what will maximise the value generated from the IP.

GOVERNANCE

INdata CRC will be an incorporated company limited by guarantee with an independent, skills-based board of directors.

INdata CRC's constitution will reflect the company's vision of building a safer and more secure nation and sharing the benefits of its work in order to be eligible for registration, and receive tax exemptions, as a registered not-for-profit organisation.

INdata CRC will draw upon the governance polices, processes and practices of the Data to Decisions CRC, which were widely regarded as exemplars in the CRC community. The CRC will commit to good corporate governance and will develop robust management and governance policies as identified in the CRC Governance and Management Guide[4], the ASX corporate governance principles and recommendations[5] and other resources provided by the Australian Charities and Not-for-profits Commission[6].

To this end, the Board will:

- establish the overall policy for the INdata CRC;
- provide strategic direction to the INdata CRC;
- oversee the financial management of the INdata CRC;
- monitor the performance of the INdata CRC Executive Team;
- ensure the project activities of the INdata CRC are consistent with the needs of its end users;
- ensure the activities of INdata CRC is consistent with its Constitutional Objects; and
- ensure the INdata CRC operates with integrity and transparency.

[4] http://crca.asn.au/wp-content/uploads/2012/05/CRCGuideC-CRC-Governance-Management.pdf

[5] http://www.asx.com.au/documents/asx-compliance/cgc-principles-and-recommendations-3rd-edn.pdf

[6] http://www.acnc.gov.au/ACNC/Manage/Tools/ACNC/Edu/Tools/MainTools.aspx

HOW WILL INDATA CRC OPERATE?

The Board composition will cover collective expertise in corporate governance, strategy development, national security, IP management, commercialisation and technology transfer, and financial and risk management.

The Board will be advised by specialist committees responsible for strategic alignment to national security needs, audit and risk management, and project investment and continuation advice.

The INdata CRC will be managed by an executive team and led by a full-time CEO. The CEO will manage the day-to-day activities of the INdata CRC and will work closely with the Board and its committees to ensure the strategic objectives are met. The CEO will require a strong background in leading complex organisations, excellent communication skills and demonstrated track record of effectively managing competing demands.

The CEO will be supported by a small team comprising administrative support functions and the following leadership roles:

Chief Technology Officer – provides direction and oversight of the research projects and education and training program. The CTO will ensure that the outputs from these programs are delivered in accordance with the INdata CRC's strategic direction and end-user requirements.

Chief Operating Officer – responsible for financial, risk, compliance and HR management, managing and reporting on performance, WHS, contract management and the delivery of administrative support services. The COO will also act as the Company Secretary.

Partnerships and Commercialisation Manager – responsible for maintaining positive relationships with the CRC's participants and securing potential new participants, as well as IP management, user trials and commercialisation activities.

Workforce Development Manager – responsible for the leadership, strategic direction and operational management of the workforce development activities of the CRC.

DESIGNED FOR SUCCESS

The INdata CRC will build on the Data to Decision CRC's (D2D CRC) existing security-cleared staff, infrastructure, significant national security experience and track-record of success. Moreover, the INdata CRC will ensure the lessons learnt from a broad range of successful CRCs are adopted. These can be summarised as follows:

01 PROGRAMS AND PROJECTS ARE DEFINED IN A "TOP-DOWN" MANNER WITH STRONG DIRECTION AND INVOLVEMENT FROM THE END-USER PARTICIPANTS

02 THE BOARD AND MANAGEMENT TEAM ARE INDEPENDENT OF PARTICIPANTS AND EMPLOYED DIRECTLY BY INDATA CRC

03 END-USER STAFF ARE EMBEDDED INTO THE CRC ON A FULL-TIME BASIS TO STEER THE PROJECTS AND ENSURE END-USER NEEDS ARE MET

04 R&D PROJECT TEAMS COMPRISE A COMBINATION INDUSTRY EXPERIENCED DEVELOPMENT STAFF AND RESEARCH STAFF TO ENSURE THE APPROPRIATE BALANCE BETWEEN INNOVATION AND DELIVERY

05 AN AGILE DEVELOPMENT METHODOLOGY IS ADOPTED WHICH INCLUDES EVALUATION TRIALS WITH END-USERS TO CO-CREATE THE CRC'S SOLUTIONS

06 THERE IS A STRONG FOCUS ON GETTING CAPABILITY IN TO THE HANDS OF END-USERS AS SOON AS POSSIBLE

07 PROJECT PARTICIPANTS ARE SELECTED BASED ON WHO CAN BEST CONTRIBUTE TO THE OUTCOMES

08 CLEAR PROJECT MILESTONES AND DECISION POINTS (INCLUDING CRITERIA FOR TERMINATION OR CONTINUATION) ARE BUILT INTO ALL PROJECTS

09 THERE IS A STRONG INTERNAL AND EXTERNAL MARKETING AND COMMUNICATIONS PROGRAM

10 COMMERCIALISATION PATHS FOR INTELLECTUAL PROPERTY (IP) WILL BE DETERMINED ON A PROJECT-BY-PROJECT BASIS BALANCING WHAT IS BEST FOR THE END-USERS AND WHAT WILL MAXIMISE THE VALUE GENERATED FROM THE IP

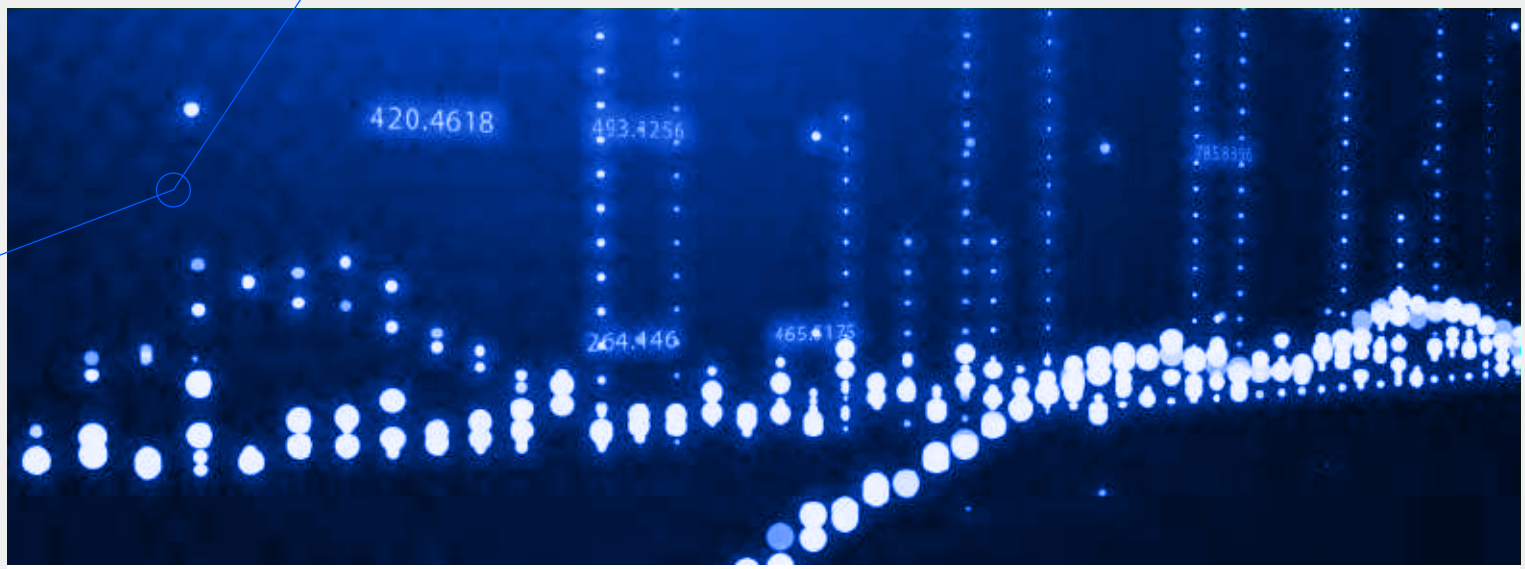
INVESTMENT REQUIRED

THE INDATA CRC HAS A PROPOSED BUDGET OF $80 MILLION OVER EIGHT (8) YEARS, COMPRISING $40 MILLION FROM THE CRC PROGRAMME AND $40 MILLION CASH INVESTED BY THE NATIONAL SECURITY COMMUNITY, COMPANIES, R&D PROVIDERS AND OTHERS.

In addition, the INdata CRC will be seeking $40 million of in-kind contributions from partners, bringing the total CRC budget to $120 million over the eight years. National security agencies will be requested to provide one staff member each to act as the primary liaison with the CRC. In addition, agencies or companies who are the primary end-user for a program will be requested to provide a technical manager to lead the relevant program. This will ensure that the program delivers to end-user needs. Other in-kind contributions sought by the CRC include background IP (products, technologies, software), access to data or other facilities (e.g. computer infrastructure) and access to operational staff (e.g. analysts, subject matter experts or capability development staff).

Term of Participation

INdata CRC will be an eight year CRC. While Participants will be expected to commit for the full duration of the CRC, participation can be reviewed on an annual basis with six months' notice of withdrawal.



THE PARTICIPATION MODEL IS AS FOLLOWS:

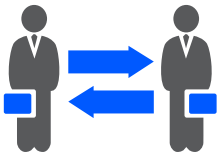
PARTICIPANT TYPE	DESCRIPTION	CASH INVESTMENT (PER ANNUM)	BENEFIT
Primary Participant	A participant that is the lead agency or company for a program. This type of participant will help shape projects and provide a staff member to lead the project ensuring their needs are being addressed.	$250k	· Ability to lead and direct projects · Ability to operationalise capabilities delivered
National security affiliate	A national security agency that will benefit from the capabilities being developed but is not directly involved in defining and executing projects.	$50k	· Ability to participate in projects · Ability to utilise capabilities delivered
R&D affiliate	Industry or research provider that may be a participant in a project (if their capabilities are relevant).	$50k	· Visibility of end-user capability needs · Ability to nominate for projects[7]

[7] Further investment (cash or in-kind investment) will be required if an R&D affiliate is selected to participate in a project

BENEFITS OF PARTICIPATION

FOR THE NATIONAL SECURITY AGENCIES, THE BENEFITS OF THE PROPOSED INDATA CRC INCLUDE:

EXPLORING THE STATE OF THE POSSIBLE IN APPLYING DATA ANALYTICS CAPABILITIES



THE DEVELOPMENT OF COMMON SOLUTIONS ACROSS AGENCY CAPABILITY NEEDS

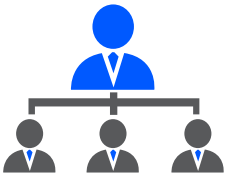
ENSURING GREATER EFFICIENCY BY REMOVING PARALLEL EFFORTS

TARGETED APPLIED RESEARCH AND INNOVATION TO SOLVE THE AGENCY'S PROBLEMS

SHARING KNOWLEDGE ACROSS AGENCIES THROUGH THE HUB AND SPOKE MODEL

AMORTISING COSTS OF INFRASTRUCTURE, STAFF AND DEVELOPMENT EFFORTS

OBJECTIVE ASSESSMENT OF EXISTING SOLUTIONS AND PROPOSALS



COORDINATING DEVELOPMENT EFFORTS AND ESTABLISHING A NETWORK OF TRUSTED PARTNERS

In summary, the INdata CRC would enable agencies to invest once, but benefit many times from the activities undertaken by the Centre.

FOR INDUSTRY AND ACADEMIC R&D PROVIDERS, THE BENEFITS MAY INCLUDE:

GAINING VISIBILITY TO CRITICAL NATIONAL SECURITY CAPABILITY NEEDS

OPPORTUNITIES TO APPLY EXPERTISE OR PRODUCTS TO SOLVE NATIONAL SECURITY NEEDS

WORKING AT THE LEADING EDGE OF DATA SCIENCE DEVELOPMENTS

LEVERAGED FUNDING TO SUPPORT R&D ACTIVITIES

CREATING AND CAPTURING NEW BUSINESS OPPORTUNITIES

COLLABORATION, NETWORKING AND PARTNERING WITH OTHER CRC PARTICIPANTS

ACCESS TO FUTURE DATA SCIENTISTS AND DEVELOPMENT OF EXISTING STAFF

POTENTIAL TO ACCESS NEW IP AND KNOW-HOW

ELIGIBILITY FOR R&D TAX BENEFITS

BID PROCESS

THE INDATA CRC WILL BE SEEKING THE INVOLVEMENT OF POTENTIAL GOVERNMENT, INDUSTRY AND RESEARCH PARTICIPANTS IN THE DEVELOPMENT OF THE BID THROUGH ONE-ON-ONE MEETINGS AND BRIEFING WORKSHOPS, WITH A VIEW TO GAIN FORMAL COMMITMENTS FROM PARTICIPANTS IN EARLY 2018

It is planned that the INdata CRC proposal will be submitted to CRC Round 20 expected to open May 2018. To meet this deadline, the following key milestones apply:

IMPORTANT DOCUMENTS AND AGREEMENTS

THE KEY DOCUMENTS THAT CRC PARTICIPANTS NEED TO BE AWARE OF ARE:

- **Term Sheet** – a document outlining the proposed terms and conditions for participation in the CRC. It will form the basis on which participation will be negotiated during the bid. The final set of agreed terms and conditions will be encapsulated in the Participants Agreement described below.
- **Commonwealth Agreement** – the funding agreement executed between the Commonwealth Government (Department of Industry, Innovation and Science) and INdata CRC Ltd. It captures the cash and in-kind commitments to the CRC and contains a detailed schedule of the activities, as well as the milestones and deliverables (outputs) to which the CRC is committed.
- **Participants Agreement** – the agreement between all financial Participants (minus the Commonwealth Government – Department of Industry, Innovation and Science). It defines the operating principles for the CRC and will encapsulate the final terms and conditions agreed to under the term sheet.

Disclaimer

For more information on the INdata CRC and how it plans to address the national security community's big data challenges, please contact:

Dr Sanjay Mazumdar / *Bid Lead*
M **0478 403 462**
E **info@INdataCRC.com.au**