CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

SUBMISSION:

An AI Action Plan for all Australians – Discussion Paper

cybersecuritycrc.org.au

Dear Sir/Madam,

Submission: *An AI Action Plan for all Australians* – Discussion Paper

I am pleased to submit the Cyber Security Cooperative Research Centre's (CSCRC) response to the Department of Industry, Science, Energy and Resources' discussion paper, *An AI Action Plan for all Australians*. We commend the Federal Government for continuing to ensure Australia's world-leading stance on innovation, one that is not undertaken purely for innovation's sake but with a view to widespread and long-term societal benefits for all Australians.

About the CSCRC

The CSCRC is dedicated to fostering the next generation of Australian cyber security talent, developing innovative projects to strengthen our nation's cyber security capabilities. We build effective collaborations between industry, government and researchers, creating real-world solutions for pressing cyber-related problems.

By identifying, funding and supporting research projects that build Australia's cyber security capacity, strengthen the cyber security of Australian businesses and address policy and legislative issues across the cyber spectrum, the CSCRC is a key player in the nation's cyber ecosystem. The CSCRC has two research programs: Critical Infrastructure Security and Cyber Security as a Service.

The CSCRC is a public company limited by guarantee and will invest $AU50 million of Australian Commonwealth Government funding and additional Participant funding over seven years to 2025 in research outcomes related to our key impact areas. The CSCRC has 25 Participants including seven Research Providers, eight State and Federal Government Agencies/Departments and 10 Industry/SMEs.

We look forward to answering any queries about this submission and welcome the opportunity to participate in future discussions regarding this very important topic.

Yours Sincerely,

Rachael Falk
CEO, Cyber Security Cooperative Research Centre
ceo@cybersecuritycrc.org.au

Executive Summary

The Cyber Security Cooperative Research Centre (CSCRC) welcomes the opportunity to provide this submission to the Department of Industry, Science, Energy and Resources (the Department) in response to *An AI Action Plan for all Australians* discussion paper. The call for views is timely and pertinent given the multi-pronged challenges and opportunities presented by Artificial Intelligence (AI).

The world is standing on the cusp of an AI-driven future. A truly transformative technology, AI offers vast opportunities, promising to unlock productivity, fuel innovation, accelerate growth and realise social and economic gains for nations, Australia included. It also has inherent qualities which could prove challenging. These qualities raise unsettling questions about ethics and the human dimensions of this technology – how citizens and existing regulatory bodies might consider mitigating risks from a technological and ethical perspective, while also unlocking competitive economic advantages.

COVID-19 has highlighted the digitally interconnected nature of the world we live in and has dramatically expedited the adoption of digital transformation across numerous sectors globally. AI has played a key role during this period, demonstrating the opportunity for Australia to better leverage existing and forthcoming technologies that bring benefit to our nation. In the United Kingdom, we have seen a number of companies quickly deploy AI-driven techniques[1] to expedite a treatment for COVID-19. In early 2020, the Australian Census-based Epidemic Model (ACEMod) utilised AI[2] to predict how COVID-19 would impact on public health control measures.

Despite these success stories, the advancement of AI and successful implementation of its technological affordances must come hand in glove with considerations about its potential

[1] Coronavirus: AI steps up in battle against Covid-19 - BBC News
[2] Can AI help in the fight against COVID-19? | The Medical Journal of Australia (mja.com.au)

security risks. Effective leveraging of AI requires extensive amounts of data, much of which is handled in the cloud and by personnel who are not cyber security professionals. Subsequently, organisations may not have the required level of cyber security maturity embedded within their processes to mitigate against a data or cyber breach. Notably, cybersecurity concerns remain front of mind for organisations who have adopted AI. In a recent Deloitte survey of 2,737 business executives across nine countries[3] (Australia included), 62 per cent of survey respondents who have overseen AI adoption within their businesses view cyber security as a major organisational risk, with almost 40 per cent admitting their organisations lack the appropriate preparatory measures to sufficiently address these concerns. Furthermore, there is a pressing need to ensure that board members of companies using AI understand the legal and ethical implications of using these technologies.

Hence, there is a clear opportunity for Australia to ensure that national advancement in AI has in-built ethical, geopolitical and cyber security considerations, and that Australia can establish itself as a leader in AI policy and practice.

Our submission responds to the following:

What is the role for government to support the uptake and use of AI technologies in Australia?

&

Do we have the right vision for AI in Australia?

The CSCRC commends the Federal Government for its proactive approach to the development and use of AI technologies. We note the 2019 discussion paper published by Data61, *Artificial Intelligence: Australia's Ethics Framework,*[4] which had the purpose of

[3] The state of artificial intelligence in business | Deloitte Insights
[4] Artificial Intelligence - Australia's Ethics Framework (industry.gov.au)

informing government's views on ethics and AI and opening up a wider discussion among the public. The subsequent commissioned report, developed by Data61 and the Department, put forth a strategic roadmap for Australia to leverage AI technological developments and position our nation to effectively capitalise on the technological affordances of AI. This proactive approach is in line with our key allies and partners, who are also putting forth views on AI 'best practice', ethics and standards.

Although AI-driven technologies in developed nations remain largely driven by industry, it should not solely be the remit of businesses to ensure they have adequately considered all risks, including cyber security risks. In this instance, government is the designated authority to establish clear domestic and international strategic perspectives on achieving AI pre-eminence through the establishment of an overarching AI strategy together with input from industry. A holistic, national strategy would inform government's approach to AI standards and together with necessary legislative and regulatory changes, send a clear signal to industry that any frameworks, principles or guidelines will remain industry-driven to ensure an economy-wide uptake of AI and continued goodwill from the business community.

In this capacity, government should also clearly communicate this strategy to industry, along with policy changes and any subsequent legislative and regulatory developments. This will ensure that industry has clear guidelines and principles to operate within, given the technological complexity of AI and the potential transformative impact it could have on their market opportunities and existing and future workforce.

However, the lack of clear guidance as to what the Australian government considers to be 'artificial intelligence' is problematic, as otherwise it risks becoming another opaque technical term which is deployed across many contexts but lacks specificity. Only once definitional clarity has been achieved can there be conceptual clarity for stakeholders. The

CSCRC submits that early consideration be given as to what technologies the government considers to be AI and what are not, with such definitional clarity provided sooner rather than later. This will help ensure government, academia and industry approach AI through the appropriate risk and opportunity frameworks. Furthermore, any definition or list of technologies that fall under an overarching umbrella of AI should be subject to annual review, given the fast-moving pace of technological development. Given Australia's longstanding relationship with our Five Eyes partners, it makes sense the government might consider drawing from their approach in the interests of alignment, a common lexicon and harmonisation.

Although the CSCRC believes the Federal Government has the right vision for AI and the nation, a comprehensive and future-focused strategy should be undertaken. This should be done while casting a cautionary eye to geostrategic competitors such as China, which has recognised the potential ability for technologies such as AI to shape future normative values and systems along with economic, geopolitical and political outcomes. Signalling its ambition to become a global AI superpower and secure an AI-driven future for the nation, in 2017, as part of China's *Made in China 2025* strategy, the State Council of the People's Republic of China published its *Artificial Intelligence Development Plan*[5] which highlights China's perspective that "artificial intelligence has become the new focus of international competition" (p. 2). The plan notes that for China to capitalise on AI's geostrategic importance and not only achieve technological pre-eminence, but maintain "social stability" over its population, it must look to "artificial intelligence development at the national strategic level, grasp firmly the strategic initiative of international competition during the new stage of artificial intelligence development, create new competitive advantage, open up new spaces of development, and effectively promote national security" (p. 2). The CSCRC urges the government to continue working alongside key

[5] Microsoft Word - A New Generation of Artificial Intelligence Development Plan.docx (flia.org), p. 2

democratic allies to establish global normative values for realising the potential within AI for all societies.

Furthermore, given that China's efforts to ensure 'social stability' have been repeatedly exposed as a form of government monitoring and control over ethnic population groups[6] through the use of AI, the CSCRC urges the Federal Government to give sober consideration to the many ethical concerns wrought by AI, ensuring the national approach to AI technologies is informed by democratic ideals and values. China is not the only perpetrator in this regard. A 2019 Carnegie Endowment for International Peace report found that repressive regimes around the world are deploying AI techniques to conduct mass surveillance over their populations,[7] including Russia and Saudi Arabia. Given Australia's proud tradition as a liberal democracy, the CSCRC rests assured that, together with key allies, the government will chart an effective course navigating these concerns while acting as global standard-bearer concerning the upholding of human rights and dignity.

How can government help ensure that AI research, including international collaboration, is undertaken safely, ethically and responsibly?

The CSCRC submits research and development will be central to ensuring Australia's leading role in AI development and recommends that the Federal Government continue to actively support Australia's vibrant research community. The CSCRC urges ongoing priority be given to the cyber security considerations associated with AI technologies through the research and development lifecycle. To that end, we recommend that government consider mechanisms to ensure AI research undertaken in Australia be developed with the 'secure-by-design' principle, so that consequent commercialisable AI products, services and

[6] How China's Government Is Using AI on Its Uighur Muslim Population | In the Age of AI | FRONTLINE | PBS | Official Site
[7] The Global Expansion of AI Surveillance - Carnegie Endowment for International Peace

solutions have security considerations ***built-in*** and are fit-for-purpose for the digital age amid ongoing cyber security threats to networks and systems.

Alongside the 'secure-by-design' principle, the CSCRC strongly urges that ethical considerations when undertaking AI research must remain front of mind, given the demonstrated bias inherent in numerous AI algorithms and systems.[8] Such biases introduce 'invisible' discriminatory practices and behaviours into AI technologies, which could have profound and disturbing human rights impacts on citizens and society alike. To mitigate this, the CSCRC recommends the Federal Government consider opportunities to grow greater awareness of Australia's voluntary *AI Ethics Principles*[9] within the research community. Furthermore, the government should explore where there is scope for various incentivisation mechanisms to ensure greater uptake of these principles by researchers. Noting that one of the principles pertains to "privacy protection and security", namely, that across "their lifecycle, AI systems should respect and uphold privacy rights and data protection, and ensure the security of data", this approach would have the corollary effect of growing the security awareness of Australia's AI research community, thereby contributing to a community-wide, cyber security uplift. On that note, consideration needs to be given to where AI research will be commercialised and utilised, in the interests of understanding the limits and end-users of any resultant AI products, services and solutions.

Lastly, the CSCRC submits international collaboration on AI research be undertaken with data and cyber security considerations in mind. As the 'lifeblood' of modern research,[10] the lucrative business model of international collaboration between research institutions is increasingly under fire for its vulnerability to foreign cyber espionage, whereby malicious cyber actors seek to steal intellectual property and gain access to valuable technology research which may have substantive impact on nations' future national security, economy

[8] This is how AI bias really happens—and why it's so hard to fix | MIT Technology Review
[9] AI Ethics Principles | Department of Industry, Science, Energy and Resources
[10] Australia is cracking down on foreign interference in research. Is the system working? (nature.com)

and sovereignty. An August 2020 ASPI report entitled *Hunting the Phoenix: The Chinese Communist Party's global search for technology and talent*[11] underscored methodologies undertaken by foreign actors to gain illicit access to technologies and conduct technology transfer. Accordingly, the CSCRC commends the Federal Government's recent efforts to establish the University Foreign Interference Taskforce and urges further consideration be given to mitigating against cyber security risks in the *Guidelines to Counter Foreign Interference in the Australian University Sector*.[12] Although the Guidelines already address cyber security as a key consideration (p. 24), requisite stakeholders might consider providing stronger incentives for Australian universities regarding these measures, noting that currently the Guidelines are not compulsory and are 'best practice' only.

How can Australia best coordinate its national research effort around areas of national priority?
&
How can we better support industry-researcher engagement?

The CSCRC is encouraged to see the focus on growing a national research effort on AI, along with other areas of national priority such as cyber security. On this front, the CSCRC submits that Australia's Cooperative Research Centre (CRC) model is globally unique, and well-suited to meeting the challenges of the digital age and leverage AI research. CRCs are collaborations between industry, government and academia, which offer the unique opportunity for Participants to bridge the gap between research and real-world applications, creating material solutions for sector-specific problems. These solutions are backed up by academic rigour and industry and government experience. CRCs drive innovation and help build Australia's capability and capacity for the future. The CRC model

[11] Hunting the Phoenix | Australian Strategic Policy Institute | ASPI
[12] Guidelines to Counter Foreign Interference in the Australian University Sector | Department of Education, Skills and Employment - Document library, Australian Government

was an initiative of the Commonwealth, established in 1990 and the CSCRC is one of more than 20 CRCs now operating across a broad spectrum of sectors. The Federal Government may wish to consider potential opportunities to establish an AI CRC, which will utilise the public/private partnership model and effectively deliver real-world research solutions for the future.

Furthermore, our organisation submits that interconnected and collaborative ecosystem models, such as the one that has been built to support the Australian cyber security sector since the 2016 *Cyber Security Strategy*, of which the CSCRC is an active member and participant, are effective building blocks to achieving comprehensive and future-focused research. The leveraging of existing capabilities across various government agencies and organisations is essential to building a robust and globally competitive sector, demonstrated by the conjoined efforts of the Australian Cyber Security Centre (ACSC), Australian Signals Directorate (ASD), the CSCRC and cyber security industry growth centre, AustCyber.

What is the best way to ensure Australians have the skills and capabilities they will need for an AI enabled future?

&

What is the best way to ensure Australian businesses have access to the AI workforce they need for an AI enabled future?

In order to effectively facilitate an AI enabled future by growing opportunities for Australians and ensuring that Australian businesses have the workforce required, the CSCRC recommends the Federal Government take a coordinated and proactive approach to growing a sustainable and holistic pipeline of talent. The *Action Plan* notes that to realise the technological affordances of AI for all of Australia along with its economic and societal benefits, that up to 161,000 AI professionals will be required for the nation by 2030 (p. 18).

Given this, the CSCRC makes several recommendations. First and foremost, we recommend that any action in this space must build upon the definitional clarity for AI the CSCRC urged earlier in this submission. A clear and shared understanding of what is meant by AI is the essential building block for progress on the human capital front, to ensure that we are training the AI professionals of tomorrow to tackle an agreed set of problems. Second, we recommend Federal Government look to global best practice strategies undertaken by our key allies and partners to tackle the human capital equation in relation to AI. For example, the UK is taking a comprehensive approach to building out a sustainable pipeline of AI professionals and ensure the UK's global position as a leader in AI. in 2018, the UK published their national AI strategy, *AI Sector Deal*,[13] which takes a multi-pronged approach to increasing AI competencies across the workforce. This strategy includes upskilling and reskilling opportunities for existing workers along with significant funding packages directed at the post-secondary and VET sectors to create more pathways to AI careers and boost funding for the research community. Gaining a deeper understanding of these approaches can inform our own, offering opportunities for Australia to draw upon existing initiatives and adapt them to our unique market conditions and capabilities.

Thirdly, the CSCRC notes the Federal Government may wish to look to existing national approaches currently underway to build future-focused workforces, in areas such as cyber security. As noted in Australia's recent *2020 Cyber Security Strategy*,[14] Australia has a critical skills shortage of cyber security professionals and there is a pressing need to build a holistic pipeline of cyber security talent. Various government programs and initiatives have been launched to meet this need, with support from industry and the post-secondary sector. Likewise, for AI, considering the skills gap, government efforts should be immediate and active, with an eye to potential and future accreditation standards for Australian AI professionals, which the CSCRC is an advocate for in the cyber security sector.

[13] 180425_BEIS_AI_Sector_Deal__4_.pdf (publishing.service.gov.uk)
[14] Australia's Cyber Security Strategy 2020 (homeaffairs.gov.au)

Lastly, any initiatives considered by government should be developed in collaboration with business, to ensure that future efforts remain responsive to the needs of industry. Anecdotal evidence from industry indicates there continues to be a skills disjunct between the demands of the market and university graduates, with an ongoing shortfall of 'job ready' technology graduates that have 'hands-on' experience. Considering this, the CSCRC urges Federal Government to consider apprenticeship models and internship programs for AI, which accelerate traditional education timeframes, equip prospective employees with practical skills and facilitate easier transitions to industry. On this front, IBM has coined the term 'new collar'[15] to describe the emergence of a new category of work roles, which typically pertain to new employment designations in the digital era – in industries such as cyber security, cloud computing and AI – which do not entail traditional education pathways and combine business critical technical and soft skills. As a signal to the market and to governments, IBM has recently launched programs and initiatives building on the apprenticeship training model. This will support the rapid uptake, at scale, of future-focused technologies by prospective job candidates, ultimately facilitating a workforce of the future.

Is there more the government can do to support responsible and human centred development and use of AI in Australia?

&

What security issues associated with AI systems should be considered?

On the former question, the CSCRC commends the Federal Government for approaching the use of AI and AI-related technologies with full consideration to potential ethical and human rights issues, demonstrated by the publication of its *AI Ethics Principles*. Likewise, the CSCRC is encouraged by government's efforts to ensure that AI development remains

[15] https://www.ibm.com/training/newcollar

human-centric, inclusive and non-biased through alignment with Australian legislative checks and balances and the global approaches of our key allies and within global fora. On that front, ensuring that the *individual* and the rights of the individual remain front and centre in privacy considerations, rather than mere providers of data to organisations, and ensuring that these considerations are guided by the *Privacy Act 1998 (Cth)* are commendable. Additionally, ongoing consideration should be given to ensuring supply chain integrity and mitigating against potential threats to Australian sovereignty, when adopting overseas AI imports which may not have been developed with the norms and values typically embedded within Australian society.[16] In this regard, Australia has the clear opportunity to build on the success of our burgeoning domestic AI sector – with Australian AI-driven companies[17] expanding their reach and experiencing market success.[18]

Regarding the latter question about what security issues associated with AI systems should be considered, the CSCRC notes that balancing and meeting public trust should remain an imperative when developing and utilising AI, both for government and industry. Public faith in AI technologies and their benefits to Australian society will erode quickly if security considerations, particularly cyber security concerns around the integrity of and unauthorised access to the data being used to inform AI, are not central to decision making and AI design thinking. As before, research and development will play a central role in protecting and securing AI technologies. That is, the ‘secure-by-design’ approach should be built into the research and development stage, to ensure that cyber security provisions for AI technologies are developed in line with current and emerging cyber security threats.

Conversely, it should be noted that AI technologies can be utilised to counteract cyber security threats at scale and hyper speed, utilising cognitive ability that currently exceeds human capacity. For example, the growing threat posed by disinformation and

[16] 201901-Feldstein-JournalOfDemocracy.pdf (carnegieendowment.org)
[17] Preparing the world for the future of work (faethm.ai)
[18] Hyper Anna - Insights. Not another dashboard.

misinformation – manipulated narratives and campaigns undertaken by a range of actors to undermine Western democracies and achieve strategic and political aims – are increasingly being facilitated by AI technologies and disseminated via the internet and social media channels. The use of 'deep fake' technology aims to manipulate public opinion and poses potential threats to political stability and security. In consideration of these novel tactics, the UK's Government Communications Headquarters (GCHQ) recently commission a report entitled, *Artificial Intelligence and UK National Security*[19] which underscored the critical need for the UK to actively implement AI capabilities into its cyber security practices to effectively respond to the growing sophistication of hostile AI activity (p. vii). Accordingly, the CSCRC submits that the Federal Government and responsible government agencies consider opportunities to leverage similar capabilities online for our unique domestic context.

[19] ai_national_security_final_web_version.pdf (rusi.org)