CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

SUBMISSION:

Data Availability and Transparency Bill 2020 – Consultation Paper

cybersecuritycrc.org.au

Dear Sir/Madam,

Submission: Data Availability and Transparency Bill 2020 – Consultation Paper

I am pleased to make this submission to the Office of the National Data Commissioner on behalf of the Cyber Security Cooperative Research Centre (CSCRC) regarding the exposure draft of the *Data Availability and Transparency Bill* (the Bill). The CSCRC commends the Federal Government for its ongoing commitment to ensuring Australia remains a prosperous, digital nation and a global leader at integrating data through the quick and effective delivery of essential services to 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 ten Industry/SMEs.

Key submissions:

The CSCRC welcomes the opportunity to provide this submission regarding key cyber security considerations relating to the exposure draft of the Bill. Such a consultation is timely and pertinent given the widespread proliferation of data and urgent need to ensure cyber secure best practices for public sector data. Globally, cyber security remains a

foremost consideration when it comes to the protection of valuable public sector data, with 16 per cent of cyber breaches in 2019/20 found to have taken place across the public sector[1]. Malicious cyber actors continue to hone tactics, state-of-the-art methodologies and strategies to access vast troves of personal data for nefarious purposes and financial gain, including illicit trade on the dark web.

There is a clear opportunity for the Australian government to act as a global exemplar in the sharing and use of government data. This can be achieved through the provision of a holistic, efficient and effective framework that modernises and streamlines the use of public sector data by relevant stakeholders, thereby ensuring Australia remains on the cutting-edge of data and privacy considerations. The CSCRC supports the Australian government's endeavour to provide rigorous and cyber secure protections around the data of individuals, to protect the rights and interests of all Australians in accordance with domestic and international human rights principles. To that end, the CSCRC commends the Office of the National Data Commissioner for its commitment to providing a whole-of-government data sharing uplift through proposed legislative reforms, the establishment of an independent regulator and other mechanisms to safeguard public sector data and ensure better delivery and access of data. This is a positive development and resonates with the aims of *Australia's Cyber Security Strategy 2020*[2], which similarly advocates for a holistic, cross-agency and departmental approach to mitigating cyber security risks across the Australian economy.

However, this is no small task. The chief mechanism for achieving this is the Australian Cyber Security Centre's (ACSC) ongoing advice to all government agencies to implement its Essential Eight baseline strategies[3] to mitigate cyber security risks. As it stands, under the *Protective Security Policy Framework* (PSPF), which is administered by the Attorney-General's Department, only the first four of these mitigation strategies are mandatory for Non-Corporate Commonwealth entities (NCCEs)[4]. This has been the case for seven years. Despite these requirements, however, the Australian Signals Directorate's (ASD)

[1] https://portswigger.net/daily-swig/the-latest-government-data-breaches
[2] https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf
[3] https://www.zdnet.com/article/asd-essential-eight-cybersecurity-controls-not-essential-canberra/
[4] file:///C:/Users/anne/Downloads/DHA%20GR%20Report%20467%20Recommendations%201-10.pdf

Commonwealth Security Posture in 2019 – Report to Parliament[5], found 73 per cent of NCCEs reported 'ad hoc' (13 per cent) or 'developing' (60 per cent) levels of maturity in their 2018-19 protective security policy framework. 'Ad hoc' represents the lowest level of maturity, with "partial or basic implementation of and management of PSPF core and supporting requirements". Those within the 'developing category' had achieved "substantial, but not fully effective" implementation. Hence, there is an urgent need for baseline cyber security uplift across the government ecosystem. While the CSCRC recognises such uplift is a key pillar of *Australia's Cyber Security Strategy 2020,* it must be assured to ensure the integrity and security of the data sharing scheme. This is essential, as the scheme must guarantee protection of the sensitive personal data of Australians that will be facilitated through such data sharing. Therefore, the CSCRC recommends the proposed data sharing scheme be promoted and enforced as rigorously as possible, to ensure adherence and compliance is achieved comprehensively across Australian government agencies, rather than in a piecemeal fashion.

The aim of harmonisation of frameworks, protocols and data sharing mechanisms, along with the privacy considerations that safeguard them is admirable. However, the data sharing scheme will fail to deliver on expected national benefits to citizens and public policy makers if harmonisation is not mandated across all government agencies. While it is understandable that it could take some time to achieve such harmonisation, there must be a concerted effort to make this a primary consideration. This will not only support the scheme's effective implementation and application, it will assist in providing data security assurance by reducing the volume of cross platform/system data sharing that is required.

The CSCRC supports the data sharing limitations touted in the Bill, which proposes authorised sharing for three key purposes (2.2.2), including the sharing of data for research and development. As an organisation that drives collaboration across research and academic institutions developing real-world cyber security solutions, the CSCRC notes there is a clear need for researchers to access public sector data that will inform evidence-driven research projects and collaborations to inform the public and policy makers. That

[5] https://www.cyber.gov.au/sites/default/files/2020-04/Commonwealth-Cyber-Security-Posture-2019.pdf

said, however, such access must be accompanied by clear and ongoing guidance that equips researchers and research institutions with the cyber security protocols, guidelines and frameworks required to ensure the safe access, dissemination and storage of that data. Thought must always be given to why data should ever be shared and what the outcome of such data sharing will be. This includes the consideration of risk and the potential ramifications of such data being shared outside of its mandated boundaries through a data breach or other means.

Concerning the data sharing principles as a risk management framework for safe data sharing (2.2.3), the CSCRC endorses the establishment of five key principles to guide the safe and effective sharing of public sector data. However, further consideration and guidance needs to be provided about how these principles can be practically implemented, reported and managed. The CSCRC recommends that consideration be given to how to effectively resource the data sharing scheme so that it is not only effective in delivery but also mitigates against inadequate oversight mechanisms, regarding cyber security. Hence, the Office of the National Data Commissioner must have robust resources to effectively regulate and enforce the scheme. Put simply, if enacted the scheme must be seen to be enforced when non-adherence occurs. While the CSCRC supports the 'graduated approach' proposed, steps must be taken to ensure the Commissioner is properly resourced to undertake investigations and, in turn, act as an effective regulator. To this end, it is also important the Commissioner plays a key public role in promoting trust and transparency within the scheme – which includes calling out breaches – and ensuring data is shared and stored securely.

The CSCRC commends the demonstrated preferred approach of adopting existing best practice approaches, through the leveraging of the data sharing principles already successfully implemented by the Australian Bureau of Statistics (ABS). In relation to the five principles, the CSCRC notes that there is scope for additional cyber security safeguards to be built into the principles, especially concerning when and where data is shared with external parties. Cyber security supply chain risks remain a persistent and credible concern in Australia. The *Australian Cyber Security Strategy 2020* aims to secure our digital economy with forthcoming guidance on 'secure-by-design' supply chain principles to be developed to ensure the security of our digital economy. Concerning this, the CSCRC

recommends the Office of the National Data Commissioner fully consider all opportunities for alignment with the Cyber Security Strategy and current advice from the ACSC[6] to ensure harmonisation wherever possible and to bolster cyber security considerations in the data sharing principles, particularly in relation to mitigating cyber security supply chain risks. Furthermore, there is scope to explore the utilisation of non-disclosure agreements (NDAs) and a possible NDA scheme for third tier supply chain partners, to build in further legally binding security protections.

Finally, the CSCRC firmly supports the Office of the National Data Commissioner for working hand in glove with existing cyber security government entities to bolster the security of the data sharing scheme. To that end, the CSCRC urges that cyber security considerations continue to be prioritised as key elements of the scheme. The 'secure-by-design' ethos is an abiding cyber security principle which puts forth a view of cyber security practices as exercises, strategies and methodologies **embedded** into processes, design thinking and legislation from the beginning, not as afterthoughts. Such an approach helps to mitigate any unintended consequences, which is especially pertinent in relation to data sharing as it remains prone to data breaches and cyber attacks. Such breaches and attacks could have serious impacts on the public trust Australian citizens have in government entities. As previously noted, while the CSCRC broadly supports the scheme and its aims, it cannot simply act as a process in theory – it must be applied as a process in action. The CSCRC, therefore, reiterates that the scheme must be seen to be enforced, which means the Commissioner should play a key public role in regulation and enforcement, which will in turn, build public trust and confidence in the scheme.

Recommendations:

- As a matter of priority, NCCEs regulated under the PSPF must take active steps to ensure their cyber security maturity meets the minimum mandated compliance level;
- Steps must be taken to ensure the Commissioner is properly resourced to undertake investigations and, in turn, act as an effective regulator;
- The Commissioner must play a key public role in promoting trust and transparency within the scheme, taking enforcement action where warranted;

[6] https://www.cyber.gov.au/acsc/view-all-content/publications/cyber-supply-chain-risk-management

- Harmonisation of cross-departmental and agency frameworks, protocols and data sharing mechanisms should be prioritised as it will help reduce cyber security risks;
- The scheme cannot simply act as a process in theory – it must be applied as a process in action.

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

Yours Sincerely,

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