Australian Research Data Commons

Submission on the Security Legislation Amendment Bill 2020

27 November 2020

The Australian Research Data Commons (ARDC) thanks the Department of Home Affairs for the opportunity to comment on the Exposure Draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020.

Background

The success of Australia depends on an efficient and effective research sector able to provide government, industry and society the best advice possible. To meet this challenge, the Australian Government has for two decades pursued the National Collaborative Research Infrastructure Strategy (NCRIS), which generates and circulates data and knowledge about our society and environment in a set of coordinated world leading infrastructure facilities.[1]

One such example is the Integrated Marine Observatory System (IMOS).[2] The IMOS currently has a portfolio of thirteen Facilities that undertake systematic and sustained observations of Australia's vast and valuable marine estate. As research infrastructure, IMOS delivers high quality marine and climate data to Australia's scientists, students, industries and other stakeholders for their use in research and operational activities. IMOS data is taken up and used thousands of times, creating impact and benefits at local, national and global scales.

Given the size of Australia relative to the rest of the world, the Government has long recognised that these types of infrastructures must be accessible, both domestically and internationally, with multi-directional sharing of data, tools and knowledge being essential.[3] [4] This is in stark contrast to previous approaches where it was important to close systems and deny access to information - when 'knowledge was power'. A system like IMOS, would have previously been unimaginable in terms of perceived risk to a country's naval defence for example. Now, with information everywhere, the power is instead in the capacity to make sense of data faster than others.[5] This requires a fundamentally different strategy to building and protecting sensemaking capabilities. Australia cannot simply collect and hoard information about areas of land, sea or space it controls only for its benefit. To do so risks others doing the same; increasingly, others will challenge any behaviour that degrades their access to that critical knowledge.[6]

---

[1] https://www.education.gov.au/national-collaborative-research-infrastructure-strategy-ncris
[2] https://imos.org.au/
[3] Australia's National Science Statement 2017
[4] Australian Government 2020 Research Infrastructure Investment Plan. p5.
[5] Alberts, David S., and Richard E. Hayes. *Power to the Edge: Command, Control in the Information Age*. Information Age Transformation Series. Washington, DC: CCRP Publication Series, 2003, p.72.
[6] What's China up to in Antarctica? | The Strategist

ARDC Response

The ARDC welcomes efforts to strengthen the robustness and resilience of Australia's research systems in light of ongoing threats; nevertheless methods to secure systems should not undermine the purpose for which they exist. The ARDC is concerned by the interventionist approach in the draft Security Legislation Amendment (Critical Infrastructure) Bill 2020 which we fear will not actually achieve the objectives of the Bill in the research sector but will certainly disrupt collaborative research. The ARDC suggests that a more effective strategy would be to modernise national infrastructure design, target capacity building, and incentivise conformance with open standards.

Particular areas of concern with the current approach include:

- The definition of the higher education and research sector does not account for the scale, complexity or diversity of the sector. This is in contrast to the approach in the Bill to other sectors, where only specific components are subject to the proposed changes, thereby limiting the scope and costs imposed upon them. The approach towards the research sector seems counter to the claim that the policy is risk-based.
- This approach is being put forward at a time when the research sector is already under acute financial pressure. This is a result of compounding factors. First, the sector has already re-allocated considerable resources in support of the national bushfires and the COVID-19 pandemic. Second, as a result of the pandemic response, the sector has seen substantial losses in institutional incomes. With additional cyber threats, and the government providing only $1.6 million for cybersecurity across the entire sector, further reduction in vital national research activity seems inevitable.
- The proposed changes do not fully leverage existing sector level initiatives, such as the Australian Higher Education Cybersecurity Service (AHECS).[7] Use of hubs such as these would better enable collective cyber resilience specifically tailored to the needs of individual institutions and assets within the sector.
- Lastly, by legislating intelligence service access to research systems (despite statements that no Personally Identifiable Information will be accessed), it is possible that other countries might be legally unable to share sensitive research data with Australian institutions.[8] Additionally, domestic and foreign researchers could become unwilling to work on systems known to pass their personal metadata to an Australian intelligence service. If either of these occur, it would mean Australian researchers increasingly need to work on offshore systems, which are more trusted by funders, researchers and data subjects to keep sensitive data private.

Recommendations

While the ARDC appreciates the urgency of the Department on this matter, it is strongly recommended that:

- A Regulatory Impact Analysis be co-developed with stakeholders and completed prior to further passage of the Bill as per previous recommendations from the Productivity Commission.[9]
- Collaborative incident response should be the preferred approach. This should aim to avoid both the punitive aspects of the proposed 'assistance' measures as well as the planned increase in red tape and regulation.
- Following development of a more collaborative approach informed by a Regulatory Impact Analysis, the Government should co-invest in capacity building led by sectoral hubs, such as AHECS. This would allow stakeholders to demonstrate their inherent willingness to protect their critical infrastructure from all hazards while also more accurately capturing the cost of uplifting cybersecurity capacity.

[7] https://caudit.edu.au/ahecs
[8] The CJEU Judgement in the Schrems II Case
[9] Productivity Commission 2012, Regulatory Impact Analysis: Benchmarking, Research Report, Canberra, p.2.

About Us

The purpose of the ARDC is to provide Australian researchers with competitive advantage through data, providing access to leading edge data intensive infrastructure, tools, services and collections of high-quality data. The mission of the ARDC is to accelerate research and innovation by driving excellence in the creation, analysis and retention of high-quality data assets.

Should you wish to discuss these or other matters in relation to the draft exposure Bill, please do not hesitate to contact Mr Adrian Burton, Director, Data, Policy & Publication Services on email ([redacted]) or telephone ([redacted]).