14 May 2021

Department of Home Affairs
By email: ci.reforms@homeaffairs.gov.au

Submission to Inquiry into Draft Critical Infrastructure Asset Definition Rules

About us

The **Allens Hub for Technology, Law and Innovation** ('the Allens Hub') is an independent community of scholars based at UNSW Sydney. As a partnership between Allens and UNSW Law, the Allens Hub aims to add depth to research on the diverse interactions among technology, law, and society. The partnership enriches academic and policy debates and drives considered reform of law and practice through engagement with the legal profession, the judiciary, government, industry, civil society and the broader community. More information about the Allens Hub can be found at http://www.allenshub.unsw.edu.au/.

The **Australian Society for Computers and Law** ('AUSCL') is an interdisciplinary network of IT and Legal professionals and academics focussed on issues arising at the intersection of law, technology, and society. It is a registered Australian charity with a charter to advance education and advocacy. AUSCL was officially launched in July 2020 by its patron, the Hon. Justice Michael Kirby. The Society has a a proud history, with its member societies being established as early as 1982. AUSCL provides a forum for learned discussion and debate through its Policy Lab, Working Groups and Events Program attracting support and engagement across Australia and globally.

The **UNSW Institute for Cyber Security** is a multidisciplinary Institute which focuses on research, education, innovation and commercialisation that has 'real world impact'. The Institute has over 60 members across each of our faculties. We are ambitious (achieving international impact), scholarly, collaborative and inclusive (acknowledging that cyber security is a new and developing field and seeking opportunities to broaden our understandings of the field by welcoming a broad range of disciplines), entrepreneurial (seeking opportunities to empower academics to be creative), diverse (embracing multidisciplinary and working as thought leaders), and generous and supportive (helping to develop and mentor early career academics, recognising vulnerable groups in society).

About this Submission

We are grateful for this opportunity for consultation on the draft critical infrastructure asset definition rules. This submission is not intended as a comprehensive response to all the issues raised in those rules, but rather focuses on topics on which our research can shed light. We thus limit our submission to the following propositions:

- The scope of what constitutes a critical infrastructure asset should be narrowed to ensure proportionality with respect to the grant of government powers contemplated by the Bill.
- In deciding what is a critical infrastructure asset, it is important to understand *network* interactions; dependencies are relevant in determining which components are critical.

Broad Scope of Definitions

The new Bill provides for extensive government powers in the context of cyber security incidents (Pt 3A). It will also impose new costs in complying with the requirements set out in Pt 2A. The rationale underlying this relates to the idea of *critical* infrastructure, giving the government a strong interest in high security standards and quick resolution of incidents. However, the justification, particularly for new government powers, becomes weaker in the context of assets whose critical status is not as clear.

For example, "critical education asset" is defined broadly as includes any university owned asset operated by a registered entity. The draft rules propose only to clarify the status of the Australian National University. Submissions made to date point out the potential breadth of this categorisation (see eg the submission on the Exposure Draft by the Group of Eight). Such broadly framed definitional scope is not proportionate when viewed against the grant of new extensive powers. For example, student hacktivism that disrupts courses may warrant a local response but not government powers of the kind set out in the Act and Bill. While Part 3A creates limits on the exercise of such powers (eg serious prejudice to social or economic stability, defence or national security; proportionality in the context of the incident), these matters are a matter of a Minister's satisfaction and are not subject to judicial review under the *Administrative Decisions (Judicial Review) Act 1977* (Cth). The definition of critical education asset should thus be narrowed to capture only those parts of university infrastructure operations that are *critical*: their short term disruption would lead to broader effects.

Similarly, the prescription of the .au country code Top Level Domain (ccTLD) as a "critical domain name system" under the Rules could have impact on 3.2 million domain names registered with .au ccTLD. Even if the definition of critical asset would not directly cover those 3.3 million domain names, it is not clear how this would operate in practice without affecting the domain names themselves, including those of small businesses and individual personal websites. As Allens Hub researcher Dr. Monika Zalnieriute has demonstrated, domain names have an expressive function. Thus, the exercise of government powers could have significant implications for the internationally recognised human rights to freedom of expression, freedom of association, non-discrimination, as well as rights to property and due process.[1] The right to privacy and data protection are also implicated in relation to domain names.[2] The human rights of marginalized groups, such as LGBTI communities, are especially vulnerable to disproportional interferences.[3] Considering the impact of government powers and policies on human rights, proportionality is a crucial element that must be satisfied for the interference on human rights to be legitimate.

---

[1] Monika Zalnieriute, 'Reinvigorating Human Rights in Internet Governance: The UDRP Procedure Through the Lens of International Human Rights Principles' (2020) 43 *Columbia Journal of Law and Arts* 197 ('Reinvigorating Human Rights in Internet Governance'); Monika Zalnieriute, 'Beyond the Governance Gap in International Domain Name Law: Bringing the UDRP in Line with Internationally Recognized Human Rights' (2020) 56(1) *Stanford Journal of International Law* ('Beyond the Governance Gap in International Domain Name Law').

[2] Monika Zalnieriute, 'From Human Rights Aspirations to Enforceable Obligations by Non-State Actors in the Digital Age: The Case of Internet Governance and ICANN' [2019] *Yale Journal of Law & Technology* 278 ('From Human Rights Aspirations to Enforceable Obligations by Non-State Actors in the Digital Age'); Monika Zalnieriute, 'Human Rights Rhetoric in Global Internet Governance: New ICANN Bylaw on Human Rights' (2020) Harvard Business Law Review(10) <https://papers.ssrn.com/abstract=3532991> ('Human Rights Rhetoric in Global Internet Governance').

[3] Monika Zalnieriute, 'Digital Rights of LGBTI Communities: A Roadmap For A Dual Human Rights Framework' in Ben Wagner, Matthias C Kettlemann and Kilian Vieth (eds), *Research Handbook on Human Rights and Digital Technologies* (Edward Elgar, 2019) 464; Monika Zalnieriute, 'The Anatomy of Neoliberal Internet Governance: A Queer Critical Political Economy Perspective' in Dianne Otto (ed), *Queering International Law: Possibilities, Alliances, Complicities and Risks* (Routledge, 1st ed, 2017) 290 ('The Anatomy of Neoliberal Internet Governance').

The scope of a critical data storage or processing asset (s 12F of the Act) proposed under the legislation is likely to have a wider impact on regulated organisations then what is intended by the legislature. The key elements in the definition tie the definition to an organisation that provides data storage or processing to a government entity (under 12F(1)), or a data storage or processing provider handling assets related to business critical data of a responsible entity for a critical infrastructure asset (12F(2) and 12F(3)). The scope of s 12F of the Act is also influenced by the business critical data definition under s 5 which is framed widely to capture (amongst other things) personal information that related to at least 20,000 individuals, information relating to any system needed to operate any critical infrastructure assets, or information relating to risk management or business continuity of a critical infrastructure asset. Also influencing the breadth of this provision is the definition of asset found in s 5 of the Act which includes a system, network, facility, computer device, computer program or computer data. "Data storage or processing provider" is potentially an all-encompassing term capturing any technology service provider used by an organisation. While organisations that provision managed services, infrastructure as a service, cyber security services, and key data systems should be treated as critical assets, modest and insignificant software as a service, or modest web based services used by employees within an organisation are not truly critical. The lack of a clear materiality level, or limitation across the entirety of a 12F of the Act to business critical data will create significant confusion and difficulty. The problem is compounded by the potential under section 5 of the Act for the law to capture personal devices used across an employee base. While it seems clear there is an intention under the legislation to address the risk of shadow IT,[4] and threats posed by unintended employee behaviour, it is difficult to imagine any information security team obtaining sufficient visibility and surveillance of their entire employee base to be able to monitor all potential data processing and handling activities.

These examples suggest that the government needs to consider how broad definitions of critical assets might reduce the proportionality of the Act as a whole, particularly in the context of new government powers.

Networks

In deciding what is a critical infrastructure asset, it is important to understand the overall *network* interactions. Graph theory describes the networks in terms of nodes ad edges, and provides an analytical framework for identifying critical elements in a network .[5] The greater the centrality of any node, the more likely it is to be critical. Graph theory can assist in identifying critical edges, which may be more vulnerable than node infrastructure. Using graph theory as a lens points to several problematic issues with the Draft Rules.

The use of content delivery (or distribution) networks (CDN) crosses telecommunications, data centres and broadcasting. In contrast to centralised data centres, CDN have a large number of servers that are distributed within a telecommunications network. Although major CDN providers such as Cloudflare, Akamai, Google Cloud CDN, Amazon CloudFront and Microsoft Azure are data centre and telecommunications customers, they create separate infrastructure with a distinct control plane. Consequently, CDN providers are also controlling critical infrastructure which overlaps with the critical infrastructure controlled by others. In the broadcasting sector, nodes are critical and edges are created purely by the nodes. This means that some broadcasters, particularly AM radio commercial broadcasters with a limited number of transmitters may also be critical. Even if those broadcasters are not designated as

---

[4] In this context, the term s*hadow IT* refers to all forms of information technology systems deployed by departments other than the central IT department or information technology used or deployed outside of and without knowledge and/or approval from the IT Department, for example use of personal devices.

[5] For example, Easley, David and Jon Kleinberg, *Networks, Crowds, and Markets: Reasoning about a Highly Connected World* (Cambridge University Press, 2010)

emergency service broadcasters, the effect of the loss of control of service may be significant. In the grocery sector, the decision that food distribution services should not be designated as critical infrastructure assets is reasonable. However, critical transport infrastructure should be considered *in this context*. For example, the fire which occurred after a fatal collision on the Stuart Highway in March 2021 has had a significant effect on the delivery of groceries in South Australia and the Northern Territory. The grocery sector is dependent on infrastructure that has no redundancy (no alternative routes). Therefore, Infrastructure Australia should focus resources on the unduplicated inputs upon which critical infrastructure in the grocery sector relies.

Yours sincerely,

Lyria Bennett Moses (Allens Hub and UNSW Institute for Cyber Security)

Monika Zalnieriute (Allens Hub)

Rob Nicholls (UNSW Institute for Cyber Security)

Marina Yastreboff and Benjamin Di Marco (AUSCL)