1 February 2022

Australian Government Department of Home Affairs
By email: CI.Reforms@homeaffairs.gov.au

Submission on Exposure Draft
Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022

About us'CI.Reforms@homeaffairs.gov.au'

The **UNSW Allens Hub for Technology, Law and Innovation** ('UNSW Allens Hub') is an independent community of scholars based at UNSW Sydney. As a partnership between Allens and UNSW Law and Justice, the 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 UNSW Allens Hub can be found at http://www.allenshub.unsw.edu.au/.

The **UNSW Institute for Cyber Security** ('IFCYBER') 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 the opportunity to make a submission on the Discussion Paper. Our submission reflects our views as researchers; they are not an institutional position. This submission can be made public.

Our main points relate to:

- the importance of accountability where government plays an increased role in security of private assets;
- independent review of Ministerial powers to make declarations under Part 6A;
- the roles of Home Affairs and the Australian Signals Directorate; and
- the data storage and processing definitions.

Clear accountability

The Bill provides, through various mechanisms including reporting, provision of information, mandatory vulnerability assessments, directions, and mandatory installation of software, for greater government involvement in the security of critical assets and systems. While this is intended to reduce risk (assuming competence and expertise in diverse assets and systems), it might also blur accountability when things go wrong. To give an example, suppose the Secretary exercises power under s 30DJ, requiring an entity to install a particular software program. If this program contains a vulnerability (unknown to the Secretary) that leads to a security exploit – who is to blame and where should any losses fall? The point here is not that risk will increase, but that *even if government involvement reduces risk overall*, the fact that government is informed of or directs some security functions complicates the question of who is responsible where something goes wrong. A similar problem arises if a vulnerability assessment conducted by a designated officer fails to identify a problem, if time dedicated to following a government direction means another threat is missed, or if reporting reveals an issue that is not followed up. It is possible that, in such scenarios, the private and public entities will each blame the other.

These issues can, in some circumstances, be clarified through additional provisions. For example, the Bill could state explicitly that organisations take responsibility for their own risk assessment programs and that this is not affected by the filing of reports. Conversely, the Bill could state that where government essentially takes control over systems (by mandatory installation of software or in the context of directions with which the organisation must comply), the government is responsible and will compensate the organisation for any harm that is causally linked to that interference on the balance of probabilities.

Clear accountability chains are not only important to allocate blame and costs where something goes wrong, they also reduce the probability of something going wrong. If entities (public or private) know that they are responsible for error, they will seek to minimise it. Where everyone feels they can point the finger elsewhere, there is little incentive for anyone to take sufficient care.

Systems of National Significance (SONS) and the Secretary's role

The Minister has broad, unchecked powers to make declarations under Part 6A. The primary check comes from the Secretary of the same department (s 52E). Given the implications for an entity becoming a SONS, entities should be able to seek an independent review. If there are security concerns, a role could be created similar to the Independent Reviewer of Adverse Security Assessments, so that a person with appropriate security clearance can be appointed.

Roles of the Department of Home Affairs and the Australian Signals Directorate (ASD)

Even beyond that context, the delegated powers of the Secretary of the Department of Home Affairs are broad. In particular, the Department will be responsible for both policy and regulation across all relevant sectors. In some contexts, where there are established relationships with industry regulators, it may be beneficial to keep the 'regulation' aspect with existing regulators.

ASD's role in the new framework is central to the enhanced security obligation provisions that apply to SONS under part 2C. The new provisions require SONS to report certain information, including installing software to facilitate reporting. Given the central role that ASD will play in the new framework, clarification of its role and its accountability is key. From whom do entities take direction? Does it make decisions? If so, are they reviewable? ASD is a statutory authority within the Department of Defence. Its accountability framework still reflects its defence origins. Information and expertise sharing arrangements exist under *Intelligence Services Act* (2001) with carve outs from certain reporting requirements and oversight. Specific provisions of the new regime permit ASD personnel or classes of personnel to be designated officers of the Department of Home Affairs for the purposes of the Act (Division 6). Designations are not legislative instruments and thus not subject to disallowance. Both this mechanism and ASD's role generally require more detail and clarification.

Issues relating to the data storage or processing sector

Definitions of 'data storage and processing' and 'critical data storage or processing asset'

Para 35 of the Explanatory Document notes that amendments to these definitions were made in response to the expressed concern of the data storage and processing industry that the current definitions in section 5 and 12F of the Act lacked clarity. Attempts to add clarity to these definitions is a laudable goal, but there remain several issues to be addressed to achieve that goal. In particular, the discussion contained in paras 29-33 does not appear to be clearly consistent with the text of the Exposure Draft.

First, 'data processing' is defined in the Explanatory Document at para 33, but this definition is not included in the Exposure Draft of the Bill – is this an oversight? This omission from the Bill adds a complicating factor to interpretation of the legislative provisions, by both industry and judges. This complication surely should be avoided if possible in an already complex legislative regime, and any definitional material should be added to the Bill.

Second, it is unclear how the changes in the Exposure Draft definitions align with the NIS Directive or the NIST standards as stated in para 31 of the Explanatory Document. The NIST definition of data processing is impliedly referenced in para 33 of the Explanatory Document, but is not incorporated into the Exposure Draft. The closest relevant NIS Directive definition appears to be that of Art 4(19):'"cloud computing service" … a digital service that enables access to a scalable and elastic pool of shareable computing resources.' However, none of this wording seems to appears in the Exposure Draft or the Explanatory Statement.

Third, para 29 of the Explanatory Document states that the amended definition provides 'additional language around the types of physical assets, such as computing systems or other physical infrastructure' used by data storage/processing services. However, the amendments to s 5 of the Act in the Exposure Draft are limited to a data processing service that 'involves the use of one or more computers'. No reference is made to other forms of 'physical infrastructure'. Additionally, purely manual processing that where a service provider merely uses a computer to email the results would likely fall under this definition. This means that the definition is extremely broad, and both industry and the government need to examine the practicalities and cost of this.

As a whole, the proposed amended definitions in section 5 seem to broaden significantly the inclusion of services under the Act, but do little to aid clarity.

The major amendment to s12F, to omit the limiting terms 'wholly or primarily' from the definition of the critical data storage or processing asset, does add clarity. However, it also broadens significantly the application of section 12F, to assets involved in purely incidental processing of data.

Both sets of amendments considerably broaden the application of the Act's provisions (save for the excision of non-commercial services from the sector definition). This may be deliberate and intended, but as this is not mentioned in the Explanatory Document, our concern is that both practical issues with implementation and cost to industry (eventually to be passed onto consumers) have not been considered in detail.

'Deconflicting' obligations

Several industry entities (eg Atlassian and Microsoft) made the point during various industry consultations that the nature of the data storage and processing sector means that it is at high risk of 'duplicative and inconsistent obligations', as they provide services across all sectors and will be required by their customers to apply sector-specific rules under the Act, as well as comply with their own sector-specific rules. Our preliminary research indicates that this is already a perceived problem with *existing* Federal and State legislative, policy, strategy and guidance material applicable to the sector.

It is welcome that para 72 of the Explanatory Document mentions these potential conflicts, at least in the limited context of the Risk Management Plan obligation. However, a positive obligation for the legislature and rule-makers to actively consider potential conflicts for horizontal providers across sectors such as the data storage and processing sector would likely bring benefits around trust, compliance and cooperation by and with industry.

Yours sincerely,

Lyria Bennett Moses

Kayleen Manwaring

Susanne Lloyd-Jones