1 March 2022

Parliamentary Joint Committee on Intelligence and Security
Via email: pjcis@aph.gov.au

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

About us

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** 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 to the Parliamentary Joint Committee on Intelligence and Security's review of the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 (the Bill). Our submission reflects our views as researchers; they are not an institutional position. This submission can be made public.

This submission sets out:

- our views of the consultation on the Exposure Draft;
- our concerns that have not been incorporated into the Bill nor addressed in the Explanatory Memorandum (EM);
- our five key themes of feedback; and
- our overall concerns about the Bill as presented.

Did you provide feedback on the exposure draft, and do you feel like consultation was inclusive and wide-ranging?

We provided a submission dated 1 February 2022 to the Department of Home Affairs (DHA) on the exposure draft of the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 (the Bill).

The consultation undertaken by DHA was focused on the industries affected by the reforms (CI Industries) and strategic in its use of facilitated town hall meetings, principally directed to critical infrastructure industries. We attended 1 of 4 town hall meetings scheduled over December, January, and early February. While a range of interested groups and individuals could participate, there was limited time available for questions. Some questions were answered in the time available. From our recollection, questions concerned the status of existing regulation in different industries, such as the finance industry, and how the new rules would impact the same or similar obligations already in operation, such as those required by APRA. Questions also queried how and when the new 'last resort' powers included in the Bill would be exercised by the DHA.

Overall, the process of consultation was well organised and strategically delivered. However, we are particularly concerned about the short time allowed between the close of submissions (1 February 2022) and the turnaround of the draft Bill (first reading on 10 February 2022). While this rapid turnaround is a tribute to the work ethic of the DHA officers responsible for the Bill, the short time frame makes it less likely that issues and concerns raised in submissions could be considered in sufficient detail.

Has your feedback been incorporated in the Bill or addressed in explanatory material?

We set out below our feedback that has not been incorporated in the Bill or has been only partially addressed.

- *The Bill does not contain immunity or compensatory provisions concerning harms causally related to the exercise of those powers exercised under s30DJ.*

  We noted that under s 30DJ, the Secretary can require an entity to install a particular software program. We explained that there was a gap in the legislation concerning what happens and who pays when things go wrong with that software. We also raised the possibility of a designated officer failing to identify a vulnerability in an assessment, or an entity failing to notice a threat due to focusing resources on compliance with a government direction, or a report revealing an issue that is not followed up.

  We recommended that additional provisions be included in the Bill which apportions responsibility for different activities between industry and government and includes appropriate compensation for any harm that is causally linked to an exercise of a power by the government.

  We note that the Bill (like the Act) contains provisions relating to immunities from actions for compensation in a range of circumstances and applying to a range of entities and individuals affected by the Bill. However, immunity from action is different from allocation of responsibility or a requirement to compensate for harm caused. Our concern thus remains unaddressed.

- *Our recommendation for independent review of the decisions of the Minister under Part 6A has not been addressed. The Bill does not provide adequate safeguards for the exercise of powers under s52E.*

  We raised a concern about the reviewability of the exercise of the Minister of Home Affairs' powers to make declarations under Part 6A concerning systems of national significance. We noted that the primary check on the exercise of that power lies with the Secretary of the DHA under s52E.

  We recommended that given the seriousness of a declaration and its potential impact on the affected entity, entities must have access to independent review of the Minister's declaration. We suggested that an independent reviewer could be appointed, like the Independent Reviewer of Adverse Security Assessments, with the appropriate security clearances in place.

  Our recommendation has not been incorporated in the Bill or addressed in the EM.

- *Our concern about the broad powers granted to the Secretary of Home Affairs, making the Secretary responsible for both policy and regulation has been partially addressed.*

  We suggested that it may be beneficial to keep the 'regulation' aspect of the reforms in the Bill with existing regulators, who have deep knowledge, experience, and expertise of regulating their industry sectors.

  The EM explains at page 46 that 'the Government intends to work with industry and State and Territory governments to identify and leverage existing regulations, frameworks and guidelines to manage risks to critical infrastructure assets, and to minimise any duplication or unnecessary burden, and to de-conflict requirements for entities with assets which fall within more than one definition of critical infrastructure asset.' We note the provisions in the Bill that support this intention, particularly that the positive security obligations in Part 2A will only apply to critical infrastructure assets that are not subject to other regulatory regimes of a similar nature.

  However, we suggest further consideration be given to identifying the actual and potential duplication, inconsistency and overlap between federal and state laws and regulation before any declarations are made for the classes of assets listed at paragraph 131 (page 30). We also suggest the government consider delegating the regulatory aspects of the Bill to existing CI industry regulators.

- *The roles of ASD and DHA have not been adequately explained and clarified.*

  We recommended clarification of the role of ASD vis-à-vis DHA and vis-à-vis affected CI industries, as some CI industries will be engaging with DHA and ASD for the first time as critical infrastructure.

  In our submission, we noted that the Secretary for Home Affairs can designate employees of ASD as employees of DHA for the purposes set out in the Bill, and that ASD has been empowered to receive and act on certain information in certain circumstances, such as under sections 30BA and 30BBA, and relevantly for SONS, under section 30DJ.

We note that the EM clarifies the role of ASD by:

- stating in most instances that ASD does not perform a regulatory or compliance role under the SOCI Act;
- noting certain documents published by ASD can be incorporated into rules;
- stating that ASD will use information obtained by it under the Bill 'to develop and maintain a near-real time threat picture, positioning it to identify threats early and provide actionable advice to industry to prevent and mitigate threats as they emerge';
- stating that '[s]ystem information and telemetry will be used by the ASD to inform an enhanced cyber threat picture and develop appropriate mitigations and advice for the entity.'; and
- noting the inclusion of provisions placing limits on the use of information transmitted to ASD under the SOCI Act.

These inclusions go some way to explaining the role of ASD. However, our concerns about its role and its accountability under the SOCI Act have not been sufficiently addressed.

We recommend that the role and accountability of ASD be explained more fully, including statements concerning who is responsible for its activities, who is responsible for its actions, who reviews its decisions and actions, and what happens when there is disagreement, or things go wrong, as described in the scenario above concerning SONS.

- *Our concerns about the data storage or processing sector have been partially addressed*

We made submissions that the definition of 'data processing' was included in the Explanatory Document but not in the Exposure Draft, which does not aid certainty. We also noted the inconsistencies between the definitions and the NIS Directive/NIST Standards. Now it appears that the definition does not appear in the new version of the Bill nor the EM. Therefore, issues around uncertainty persist.

Despite the claim in the new EM that the definition excludes any manual data processing, we do not believe that the current definition in the Bill does that. We submit that our example provided in our previous submission that 'purely manual processing …where a service provider merely uses a computer to email the results' would still likely fall under this definition. Additionally, the definitions in the Bill do not include additional language to clarify the definition of 'other physical infrastructure' (mentioned in the Explanatory document) outside of computers.

We noted that the amendment to 12F significantly broadened the application of section 12F assets, some of which are only incidental to the processing of data. We expressed concern that the broadened definitions would raise practical issues with implementation and cost to industry, which would eventually be passed on to consumers. The retention of the 'wholly or primarily' limiting factor, and the addition of the 'business critical' requirement, does keep the definition narrower, although this may raise issues around interpretation of these requirements.

- *Our concerns that the data storage or processing industry was at high risk of duplicative and inconsistent obligations has been partially addressed.*

  We note at page 46, the EM explains that 'the Government intends to work with industry and State and Territory governments to identify and leverage existing regulations, frameworks and guidelines to manage risks to critical infrastructure assets, and to minimise any duplication or unnecessary burden, and to de-conflict requirements for entities with assets which fall within more than one definition of critical infrastructure asset.'

  However, our recommendation that a positive obligation be included for the legislature and rule-makers to actively consider potential conflicts for horizontal providers across sectors has not been incorporated in the Bill or addressed in the EM.

What are your five key themes of feedback on the Bill?

Our five key themes of feedback are:

- *Clearer accountability and transparency*

  Accountability frameworks must be explained better and, in more detail, including accountability around government and industry engagement. Accountability should also be embedded in the operation of the Act, which includes making government liable for harms caused by its interventions.

  Transparency about decisions must be a priority, alongside contestability of decisions with significant impact on organisations. It is therefore essential that government adopts an open and transparent stance to the exercise and impact of its new powers.

  We note the review mechanisms for rules and declarations in the Bill, such as section 30AM and section 52E. We also note that parliamentary review is embedded in the Secretary's review of the rules under section 30AM(6), but not the review of declarations of systems of national significance. We further note the obligation on CI industries to review their risk management and incident response plans as specified in the Bill.

  However, there needs to be transparency around industry and government engagement and cooperation beyond the consultation for the current legislative reform process. For this reason, the mechanisms and processes of engagement should model good governance, including opening less operationally sensitive processes to the public, conducting regular reviews, and making information about industry and government cooperation publicly available.

- *Avoiding duplication and inconsistency*

  Duplication and inconsistency with existing law and regulatory frameworks is a major concern of CI industries, many of whom are operating in heavily regulated sectors of the economy. Avoiding inconsistency and duplication needs to be expressed as a positive obligation on the legislators and rule-makers, and decision makers under the SOCI Act. We note the efforts to address this issue contained in the Bill.

- *Responsiveness must be comprehensive and proactive*[1]

  Recognition of the ongoing regulatory relationship with CI industries once the reforms are operationalised is a singular issue of immense importance to the success of the critical infrastructure reforms, especially the positive security obligations framework and the enhanced security framework for systems of national significance. Efforts to improve industry cooperation should be an ongoing priority of government. The government would benefit from collaborative engagement with industry on aspects of the operation of the Bill, especially around the newer powers contained in the Bill, such as the expansive government assistance powers. To assist these efforts, consideration of the lessons from the reform process and how they can be implemented into the ongoing reform process and operationalising of the legislation would be valuable for industry and government.

- *Reliance on industry expertise*

  Many of the industry sectors now considered critical infrastructure already operate within longstanding regulatory frameworks. Their knowledge and expertise of their sector, combined with their existing obligations and regulatory relationships, make industry's input crucial to understanding the nature of sector specific risks and generating potential solutions and innovations to those risks. We encourage government to continue to actively engage with industry experts on the matters under consideration.

Do you think the potential regulatory impact has been captured accurately?

The regulatory impact of this legislation will be significant on the selected critical infrastructure sectors. It will create unique obligations and risks for systems of national significance. The regulatory impact will continue beyond the reform process, as the legislative scheme creates a mutually dependent, ongoing relationship between government and CI Industries.

The Bill contains a hybrid approach to industry regulation, featuring a mix of technical rules, legal obligations, and other regulatory mechanisms. It has the potential to offer greater flexibility and efficiencies to both industry and government. However, to assess its ongoing impact, measure its success and manage its challenges, both industry and government must be committed to regular, transparent, and accountable review of the scheme, along with a review of the exercise of the new powers. We note the provisions for review in the Bill as presented but reiterate the importance of the nature of the review of the scheme.

On balance, do you support the Bill in its presented form, recognising the risks facing critical infrastructure assets in Australia?

On balance, we do not support the Bill in its presented form until our stated concerns are addressed. While we appreciate the risks facing critical infrastructure assets in Australia, it is imperative that this legislation is the best possible version of reform it can be. Affected entities need time to litmus

[1] For a discussion of 'comprehensiveness' and 'proactiveness' based on the work of Philip Selznick, see Seung-Hun Hong and Jong-sung You, 'Limits of regulatory responsiveness: democratic credentials of responsive regulation' (2018) 12 *Regulation & Governance* 413-427, 418-420, cited in Karen Lee and Derek Wilding, 'Towards Responsiveness: Consumer and Citizen Engagement in Co-Regulatory Rule-Making in the Australian Communications Sector (2021) 49(2*) Federal Law Review* 272-302, 280-281; see also, Karen Lee, *The Legitimacy and Responsiveness of Industry Rule-Making* (Hart Publishing, 2018).

test these reforms in their business systems and provide feedback to government on what it looks like in practice, where the gaps are and what the costs might be. The government needs to consider how it might clarify and better explain the safeguards and oversight attached to the exercise of the powers under this Bill.

The Bill contains new expansive powers and unfettered discretions for the Minister of Home Affairs and the Secretary of the Department of Home Affairs, as the responsible regulator for the operational aspects of the legislation. The Bill also contains an expanded yet opaque role for ASD that has not been adequately explained in terms of its role, responsibilities, and accountability. The Bill contains broad definitions of industries and associated assets, impacting a vast number of businesses and entities across the Australian economy.

Given that the parliament has already passed the most urgent aspects of the reform agenda, it is now imperative that this part of the process - the part that falls most heavily on the affected industries - is given ample time for deliberation, so that the concerns of the entities on whom the government is dependent (CI Industries) for operationalising the reforms are adequately responded to.

Yours sincerely,

Lyria Bennett Moses

Susanne Lloyd-Jones

Kayleen Manwaring