Submission to the Parliamentary Joint Committee of Intelligence and Security

Review of the Cyber Security Legislative Package 2024

Outline and Summary

Thank you for the opportunity to make a supplementary submission to the public consultation on the proposed Review of the Cyber Security Legislative Package 2024 ("the Package"), comprising of the Cyber Security Bill 2024 (Cth), the Intelligence Services and Other Legislation Amendment (Cyber Security) Bill 2024, and the Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024.

This submission has been prepared by the authors in their capacity as Fellows and representatives of the Social Cyber Institute (SCI), a non-profit organisation with the mandate to create new social science insights to complement technology in the fight for a more secure cyberspace. However, the views expressed below are entirely those of the authors and are not representative of the SCI, their institutions or any other government, organisation or agency.

This submission will touch on only certain proposals contained within the Package. This does not indicate an agreement or rejection of any of the other proposals contained within the Package.

Cyber Incident Review Board

The Cyber Security Bill 2024 would also introduce a new body known as the Cyber Incident Review Board (CIRB), comprised of members appointed by the Minister[1] and assisted by an Expert Panel appointed by the CIRB.[2] The CIRB would be an independent body[3] tasked with reviewing incidents which meet the threshold criteria in section 46(3) such as scale of impact, novelty of techniques, and/or likely to be of serious concern to the Australian people. The Board is then vested with powers to gather information relevant to a review,[4] as well as circulating draft reports to affected stakeholders ahead of the publication of final reports.[5] Final reports cannot apportion blame or find liability.[6] Final reports must be publicly published,[7] though a regime exists for shielding certain 'sensitive review information' if it meets the criteria in section 53(2).

The Government is to be commended on moving to establish the CIRB. Having publicly available reports on the results of reviews post-significant incidents will enable all stakeholders to better prepare their cybersecurity posture and conduct internal diligence as to their risks and vulnerabilities. The removal of apportionment of blame or findings of legal liability from the review process is also very welcomed, as it should facilitate the cooperation of impacted entities on exhibiting candour and truthfulness in their dealings with the review.

There are however two problems with the proposed legislation establishing the CIRB.

---

[1] Cyber Security Bill 2024, s 61.
[2] Ibid, s 70(2).
[3] Ibid, s 63.
[4] Ibid, ss 48 and 49.
[5] Ibid, ss 51 and 52.
[6] Ibid, s 52(4).
[7] Ibid, s 52(6).

The first is the requirement for the Minister to approve the draft terms of reference of a review, which indirectly will include the appointment of experts appointed from the Expert Panel to assist the review.[8] This requirement is not only outlined in section 46(2)(c), but also as a Note to the "independence of the CIRB under section 63 (where the CIRB otherwise 'has complete discretion in the performance of the Board's functions and the exercise of the Board's powers').

Whilst this provision was perhaps included with the best of intentions, the operation of the CIRB cannot be allowed to be subject to such an obvious fettering of power. Ministerial intervention in the operations of any independent body obliterates any notion of independence. For a contemporary example, in the recent review report of the *Australian Research Council Act 2001* (Cth) released last year, it was said that '[i]n every iteration, Ministerial interventions have drawn international attention, and placed at threat the capacity of Australian researchers to form research links with international university and industry collaborators'.[9]

It is thus entirely possible to imagine a scenario where the CIRB wishes to press ahead with a review into a cyber security incident but is prevented from doing so by a Minister who – whether with noble or malign intention – refuses to approve the Terms of Reference for that review. Another Minister might otherwise delay approving the terms of reference to a point that renders the review pointless.

The Minister should not be clothed in power to frustrate the operations of what is otherwise an independent body. It further seems an anachronistic requirement for an environment like cybersecurity, operating with so much volatility and change. Rather, the Minister should either not have any involvement in the setting of the Terms of Reference or should merely be "advised" of the commencement of the review so that the Minister can otherwise discharge their functions.

Recommendation 1: Section 46(2)(c) of the Cyber Security Bill 2024 should be removed in its entirety.

Recommendation 2: If section 46(2)(c) of the Cyber Security Bill 2024 is not removed, it should be amended to feature words to the effect that a review may be conducted 'if the Minister has been advised of the terms of reference for the review'.

The second problem with the CIRB provisions is also related to the establishment of the Terms of Reference. There is no doubt that the members of the CIRB selected by the Minister will be experts in cybersecurity, law, corporate and strategic governance, and other vital skills. Yet it is entirely possible that the CIRB may encounter an incident into which they wish to conduct a review, but they may be unaware of novel or unique forms of cyber risk which ought to be included in the terms of reference for the review.

Section 70(3) mandates that at least one member (if not more) of the Expert Panel must be appointed for every review, 'in writing and in accordance with the terms of reference'. However, this means that the appointment of experts comes after the settling of the terms of reference. Whilst it is entirely permissible for the CIRB to seek to amend the terms of reference after experts have been appointed, this again – under the current proposed iteration of the Cyber Security Bill 2024 – would require the Minister's approval. It seems entirely inefficient and unnecessary for the CIRB to establish a term of

[8] As the appointment must be 'in writing and in accordance with the terms of reference'.
[9] Margaret Sheil, Susan Dodds, Mark Hutchinson, *Trusting Australia's Ability: Review of the Australian Research Council Act 2001* (Report, 20 April 2023) <https://www.education.gov.au/higher-education-reviews-and-consultations/resources/trusting-australias-ability-review-australian-research-council-act-2001>.

reference, seek Ministerial approval (which ought not be required in any event) and only then be able to discuss the review with the Expert Panel.

Instead, the Bill should be amended to permit the Chair of the Board to consult with members of the Expert Panel to assist in framing the issues to be included in the terms of reference. This includes during a review which is "in flight" and may uncover new information or evidence which requires the appointment of additional experts and/or a change in the terms of reference.

Recommendation 3: The Cyber Security Bill 2024 should be amended to include section 70(6), which could include words to the effect that 'For the avoidance of doubt, the Chair of the Board may communicate with any member of the Expert Panel for the purposes of establishing or amending the terms of reference for a review'.

Introduction of data storage systems to the *Security of Critical Infrastructure Act 2018* (Cth)

Schedule 1 of the Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024 will introduce changes to the *Security of Critical Infrastructure Act 2018* (Cth) (SOCI Act) to include a provision which would include "data storage systems" as part of any defined critical infrastructure asset.

According to the Explanatory Memorandum, the amendment has been made because of 'a growing number of cyber incidents impacting non-operational data storage systems held by critical infrastructure entities'.[10] Entities which provide 'a data storage or processing service' for business-critical data, where their client is an entity of the Commonwealth, States or Territories, or a body corporate, are already captured as 'critical data storage or processing asset',[11] making them by default a 'critical infrastructure asset'[12] and subject to obligations of those assets under the SOCI Act. However, only where a data storage system meets the requirements under the proposed section 9(7) of the SOCI Act will be considered "part of" the critical infrastructure asset. This raises two distinct but overlapping problems with the proposed coverage of the new section 9(7).

Firstly, the term "data storage system" is not defined either by any Acts in the Package, nor in the SOCI Act itself, meaning any interpretation of the Act must rely on that word's natural meaning.[13] The term 'data storage' is defined as 'data storage that involves information technology, and includes data back-up'.[14] 'Data storage device' is also defined, meaning 'a thing (for example, a disk or file server) containing (whether temporarily or permanently), or designed to contain (whether temporarily or permanently), data for use by a computer'.[15] Therefore, a data storage system is likely to be construed as a system involving information technology that stores data.

Yet, despite the Explanatory Memorandum making clear that the concern of Parliament is "non-operational" systems containing 'large quantities of both personal information and other business

[10] Explanatory Memorandum, Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024, 7 [17].
[11] SoCI Act, s 12F(1).
[12] Ibid, s 9(1)(d).
[13] *Project Blue Sky Inc v Australian Broadcasting Authority* (1998) 194 CLR 355, 381-382; *Alcan (NT) Alumina Pty Ltd v Commissioner of Territory Revenue* (2009) 239 CLR 27, 46-47.
[14] SOCI Act, s 5.
[15] Ibid.

critical data',[16] neither the size nor the state of operability of the data storage system are one of the conditions recognised by the proposed section 9(7).

This is incredibly problematic, as the provision is arguably broad enough to capture every conceivable form of data storage used in conjunction with a critical infrastructure asset. For example, not only will a data storage system include a server or network containing business-critical information, but any mobile device or USB drive held by an employee of that asset. So long as the threshold tests contained in the proposed section 9(7) of the Act are met, then the storage system will be captured. This would then impose a mass of cybersecurity obligations (registration, notification and critical risk management plans[17]) on the owner and/or operator of that critical infrastructure asset to secure every possible 'data storage system' that they own or operate containing business critical data.

If that is not the intention of Parliament, the broadness of that provision could be addressed by permitting the Minister to "read down" or exclude certain data storage systems from being captured by the provision through the promulgation of an appropriate Rule.

If however it was the intention of Parliament to capture every possible form of data storage owned or operated by a critical infrastructure asset, these owners and operators of critical infrastructure assets will need to be rigorously informed of their obligations in this regard as part of the implementation of this legislation.

Recommendation 4: That the Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024 be amended to include a new subsection 9(8), containing words to the effect that 'Section 9(7) does not apply to a data storage system specified in the rules'.

Recommendation 5: If that recommendation is not adopted, that the government consider a robust engagement strategy surrounding this provision as part of the implementation and commencement phase of this legislation.

Secondly, the provision at section 9(7)(a) requires that the entity 'owns or operates the data storage system', at which point the entity assumes responsibility under the SOCI Act for that data storage system.[18] This does not adequately reflect the common practice of critical infrastructure assets to "outsource" their data storage or processing to another party and risks contractual disputes over that responsibility.

Consider Asset A, which contracts with Service Provider B to host a cloud environment (the "data storage system") for operational and business-critical data. Whilst Service Provider B may well be counted as a critical infrastructure asset (by virtue of ss 9(1)(d) and 12F of the SoCI Act) and be the responsible entity for that system, Asset A now also incurs obligations as the responsible entity for that system because they meet the requisite conditions under section 9(7).

[16] Explanatory Memorandum (n 10).
[17] Ibid, Pts 2, 2A and 2B.
[18] Saying 'the responsible entity for the main critical infrastructure asset is responsible for data storage systems that they own or operate': Explanatory Memorandum (n 10) 9 [31].

The note to the proposed section 9(7) supports that interpretation, making it clear that the new "operating" party of a data storage system will incur the obligations under the SOCI Act in relation to that system, including registration, risk management and notification.[19]

Recommendation 6: That the wording of the proposed section 9(7) of the SOCI Act, amended by the Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024, be changed to include words to the following effect:

> *If, under this section, an asset is a critical infrastructure asset, then a data storage system in respect of which all of the following requirements are satisfied is taken to be part of the critical infrastructure asset (unless that data storage system is already a critical infrastructure asset):*

Managing consequences of impacts of incidents on critical infrastructure assets

Schedule 2 of the Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024 will extend information-gathering powers of the Minister under the SOCI Act to "incidents". The amendments include changing the objects of the Act (to now include 'serious incidents relating to critical infrastructure assets'), changing the response from 'a cyber security incident' to 'an incident (including a cyber security incident)' and various ancillary amendments to reflect the change in statutory language.

Parliament's intention appears to be to enshrine the Cyber and Infrastructure Security Centre's policy position of taking an "all hazards" approach to cybersecurity in the SOCI Act. That intention is very laudable and reflects a contemporary understanding of the geopolitical and transnational nature of threats to which the SOCI Act is directed. That much is clear from the Explanatory Memorandum, which stipulates the current Act does not – and should – apply to 'physical incidents like terrorist attacks and natural incidents such as floods or bushfires'.[20]

That said, the language of the amendments lacks specificity. For example, section 8G of the SOCI Act already establishes what are the relevant impacts of a hazard (and now an "incident"), and ties them to the availability, integrity, reliability of the asset and/or the confidentiality of information stored by or about the asset. Whilst a terrorist attack or bushfire could certainly cause a relevant impact, there are numerous other incidents which would be captured under this scheme:

- Power failure or damage to supporting infrastructure
- Acts by a malicious insider or malign/negligent employee
- Acts of foreign interference, espionage or sabotage
- Criminal damage
- A class action lawsuit

In effect, it is the highly subjective nature of the Minister's interpretation of section 35AB(1)(d) that is a problem.[21] Under the current regime, the Minister must simply be satisfied that no existing regulatory system of the Commonwealth, a State or a Territory could be used to provide a practical and effective response to a cybersecurity incident. That is not likely to be much of a challenge given the paucity of governmental agencies with a remit to operate in that field.

---

[19] Explanatory Memorandum (n 10) 9 [32].
[20] Explanatory Memorandum (n 10) 11 [38].
[21] Proposed SOCI Act, s 35AB(1)(d).

Once the amendments apply the regime to all incidents, the assistance powers in Part 3A of the SOCI Act – already considered a significant intrusion by government into the autonomy of private corporations in this country – would allow the Minister to authorise the Secretary to intervene in any incident that threatens a critical infrastructure asset. In effect, this legislation operates as a "switch" to permit the Home Affairs Minister to intervene in matters better left to the Australian Federal Police, State or Territory Police, or ASIO, or indeed any other organisation better placed to respond to that incident.

Where a Minister is 'satisfied' of a certain set of circumstances as existing, a remedy is not merely available out of preference for a different result.[22] Accordingly, the Home Affairs Minister may quite innocently reach the desired level of satisfaction that another agency of the Commonwealth, a State or a Territory cannot provide a 'practical' or 'effective' response to that incident, given the Home Affairs portfolios experience and expertise with critical infrastructure. In turn, this creates a significant jurisdictional risk of the Minister interfering with the operations or activities of other regulatory agencies across the Commonwealth.

Recommendation 7: That – if the government intends to retain Schedule 2 of the Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024 in its current form, the wording of section 35AB(1)(d) of the SOCI Act ought to amended to include words to the following effect:

> *(d) no existing regulatory system of the Commonwealth, a State or a Territory could be used to provide a practical and effective response to the incident, or is in any other way more appropriate to respond to the incident.*

Use and disclosure of protected information

The Package makes changes to the SOCI Act and the *Intelligence Services Act 2001* (Cth) regarding the protection of certain information.

The Intelligence Services and Other Legislation Amendment (Cyber Security) Bill 2024 incorporates the "limited use" provisions from the Cyber Security Bill 2024 to cover information provided to the Australian Signals Directorate (ASD) as part of responding to or dealing with a cyber security incident.

Firstly, the Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024 changes the definition of "security" in section 5 to align with the same definition in the *Australian Security Intelligence Organisation Act 1979* (Cth). That amendment is wholly supported, ensuring a more consistent interpretation across all critical infrastructure assets and entities as to the nature of what "security" is directed towards.

That amendment is practical and strongly supported by the authors.

Secondly, section 29(2) of the Cyber Security Bill 2024 prohibits a 'designated Commonwealth body' from using ransomware reports for investigations or prosecution activity, unless the allegation relates to a failure to report ransomware payments or the commission of a crime.[23] Section 32(2) renders that information inadmissible in proceedings other than Royal Commissions or writs of mandamus in the Federal jurisdiction. A similar structure of protection and inadmissibility also applies to information

[22] *Minister for Aboriginal Affairs v Peko-Wallsend Ltd* (1986) 162 CLR 24, at 47–8; see also *House v The King* (1936) 55 CLR 499; *Minister for Immigration and Citizenship v Li* [2013] HCA 18.
[23] Section 30(3) of the Cyber Security Bill 2024 also prohibits secondary or derivative use of that information.

voluntarily provided to the National Cyber Security Coordinator (NCSC) under sections 39(3), 40(3) and 42(2) of the proposed Cyber Security Bill 2024.

The limited use provisions are appropriate and well-targeted. However, there remains an exclusion for information sharing for contraventions 'of a law that imposes a penalty or sanction for a criminal offence'.[24] Similar exclusions apply to information and reports in the hands of the CIRB.[25] The Explanatory Memorandum makes clear that this was never intended to be a "safe harbour" regime; i.e., one where impacted entities may disclose information to the NCSC, ASD or other government entities without incurring potential legal liability for their conduct (such as not enacting cybersecurity controls).[26]

That statement is largely at-odds with public reporting around the impact of the Bill.[27]

Further, the lack of safe harbour is problematic when considering that the aim of the "limited use" provisions was to encourage impacted entities to be more fulsome and transparent in sharing information with the NCSC and ASD. The notion that members of boards and directors of medium to large-scale companies – those most likely to be impacted entities in cyber incidents – may still face criminal prosecution is likely to hamper this regime. For example, section 184 of the *Corporations Act 2001* (Cth) provides for criminal offences for officers of companies that are reckless or dishonest in discharging the obligations of their appointments. If provision of information to the NCSC and/or ASD could provide evidence for a charge under that Act, the application of "limited use" provisions is unlikely to encourage companies to be more forthcoming than they are now.

Therefore, there should be a statutory statement – such as an amendment to the "Simplified outline of this Part" in section 33 – that these provisions are not the same as "safe harbour", which has been mentioned significantly in media reporting surrounding the Package. There will also need to be significant education and improvement to the national cybersecurity narrative around the limited use provisions during the implementation phase of this legislation.

[24] Cyber Security Bill 2024, ss 30(2)(b), 30(3)(b), 38(2)(b), 39(3)(b), and 40(3)(b).
[25] Ibid, ss 55(2)(b) and 56(3)(b).
[26] Explanatory Memorandum to the Cyber Security Bill 2024, at 7, 54, 68 and Attachment B.
[27] Greg Austin, 'Forgiveness or punishment? The government's proposed 'safe harbour' laws send mixed messages on cyber security', *The Conversation* (online, 22 November 2023) <https://theconversation.com/forgiveness-or-punishment-the-governments-proposed-safe-harbour-laws-send-mixed-messages-on-cyber-security-218025>; Ange Lavoipierre, 'Cyber ransom payments will need to be disclosed by businesses under new laws', *ABC News* (online, 30 July 2024) <https://www.abc.net.au/news/2024-07-30/cyber-ransom-payments-new-laws-before-parliament/104113038>; Paul Smith, 'Business to get cyber "safe harbour" protections' (online, 17 September 2024) <https://www.afr.com/technology/business-to-get-cyber-safe-harbour-protections-20240916-p5kazn>; Daniel Croft, 'Australia's first standalone Cyber Security Act to make ransom payment reporting mandatory' (online, 9 October 2024) <https://www.cyberdaily.au/government/11211-australias-first-standalone-cyber-security-act-to-make-ransom-payment-reporting-mandatory>; Daniel Croft, 'Industry responds to Australia's Cyber Security Act' (online, 11 October 2024) <https://www.cyberdaily.au/government/11228-industry-responds-to-the-australias-cyber-security-act>.

Recommendation 8: That section 33 of the Cyber Security Bill 2024 be amended to include a statement after "Information voluntarily provided under this Part may only be recorded, used and disclosed for limited purposes" to the effect that information voluntarily disclosed under Part 4 may still be admissible in certain legal proceedings and/or for purposes of determining liability.

Recommendation 9: That the government consider a robust engagement strategy surrounding this provision as part of the implementation and commencement phase of this legislation.

Presumption of significance

There is also a matter regarding the timing of providing information to the NCSC voluntarily. Section 35(2) of the Cyber Security Bill 2024 provides that an entity may voluntarily provide information NCSC if the incident 'is' or 'could reasonably be expected to be' a significant cyber security incident as defined in section 34. However, at the time of doing so, an entity may not have sufficient information on the incident to know conclusively whether it falls into one of those two categories. Whilst a presumption exists under section 35(4) that certain types of incidents will be a 'cyber security incident', there is no such presumption for section 34 for a '**significant** cyber security incident' (emphasis added).

The result is that an entity may – in good faith and with the fullness of belief in the protection of the information so provided – give information voluntarily to the NCSC that subsequently loses its legal protections because it was the incident was not 'reasonably expected' to be a significant cyber security incident. Whilst the NCSC is provided a presumption to collect that information for the purposes of assessing whether it falls into that class,[28] affected entities are not.

Recommendation 10: That the Cyber Security Bill 2024 be amended to include a new section 35(6), which creates a rebuttable presumption that covers the circumstances where an impacted entity can presume that a cyber security incident is 'significant'. One such example could be if the incident had a 'relevant impact' defined by section 8G of the SOCI Act.

Time for consultation

As an aside, the authors have noted that the introduction of the Package to Parliament and First Reading Speech occurred on 9 October 2024. It was referred to the PJCIS that same day, with the requirement that submissions be lodged no later than Friday 25 October 2024.

With the greatest of respect, the introduction of a mammoth undertaking of legislative amendments such as the Package – with significant implications for businesses in terms of cost and time – whilst providing only twelve business days for public consultation is simply not appropriate. No doubt the PJCIS will receive submissions only from the most dedicated and keenly eyed stakeholders, capable of digesting three complex Bills and synthesising their position in such a short timeframe.

That position is made worse by the amount of time the government has had to consider its own position. According to the Explanatory Memorandum, the Package stems from a Consultation Paper issued from December 2023 to March 2024, and 'targeted consultation' from 4-11 September 2024. The Albanese Government has therefore had at least 222 days – from 1 March to 4 September 2024 and again from 11 September to 9 October 2024 – to consider how it would draft this legislation. Seeking detailed industry and stakeholder feedback on this proposed legislation in only two weeks is

[28] Cyber Security Bill 2024, s 36(2).

incongruent behaviour by a government that seeks to champion its "extensive consultation" with industry over cybersecurity.[29]

The proposed amendments provided by the Package represent a fairly thin slice of the overall promises delivered in the 2023-2030 Cybersecurity Strategy. We therefore look forward to the Albanese government bringing forward legislation as a priority to tackle the other pressing issues in that Strategy, including mis/disinformation, privacy reform and Departmental/industry collaboration.

Conclusion

Thank you for the opportunity to make this submission.

Social Cyber Institute

Corresponding author: [redacted]

[29] Tony Burke, 'Government Introduces Landmark Cybersecurity Legislation' (Media release, 9 October 2024) <https://www.tonyburke.com.au/media-releases/2024/government-introduces-landmark-cyber-security-legislation>.

Annexure – Names and Affiliations of Contributors

Professor Greg Austin – Senior Fellow and head of the Program on Cyber Power and Future Conflict with the International Institute for Strategic Studies (IISS); Professor of Cyber Security, Strategy and Diplomacy with the University of New South Wales Canberra

Dr Brendan Walker-Munro – Senior Lecturer (Law), Southern Cross University; Adjunct Expert Associate, National Security College, Australian National University

Dr Adam Turner – Google Cloud Consulting: Sessional Teaching Academic at Macquarie University's Department of Security Studies and Criminology

Mr Adam P. Henry – Adjunct Lecturer at University of New South Wales Canberra Cyber; Co-Lead of the Australian Chapter for the Cybersecurity Workforce Alliance (CWA); Director at Henry Strategic