PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

Advisory report on the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018

Parliamentary Joint Committee on Intelligence and Security

September 2021
CANBERRA

ISBN 978-1-76092-295-5 (Printed Version)

ISBN 978-1-76092-296-2 (HTML Version)

Foreword

Australia faces a very serious and rapidly deteriorating cyber security environment. It demands both a swift and comprehensive response. As this report sets out, the Committee does not believe both can be done at the same time in the same bill. If the Parliament seeks to achieve both in the same process, it may achieve neither. This is due to the inherently complex nature of the challenge and the proposed response to it, and the extraordinary and unusual economic climate we find ourselves in.

The Committee received compelling evidence that the pervasive threat of cyber-enabled attack and manipulation of critical infrastructure assets is serious, considerable in scope and impact, and increasing at an unprecedented rate. This threat requires a rapid response. However, there is significant disagreement between industry and government on the exact response required.

The scope of the proposed framework in the SOCI Bill is broad and virtually all witnesses before the inquiry supported the objectives of the legislation. However, the proposed framework has an inherently uncertain regulatory cost because much of the regulation is to be designed and defined in legislative instruments, rather than in the primary legislation. The uncertain obligations and costs imposed by the Bill would apply to Australian businesses in the context of an already fragile economy beset by lockdowns and other impacts of the COVID-19 pandemic. This environment has made it difficult for industry to fully engage in the consultation process and even more wary about the outcomes of it. As a result, many have called for the entire Bill process to be paused. Although sympathetic to these calls, the Committee does not believe that pausing the entire bill is the responsible course of action.

The Committee also faced constraints on its ability to undertake meaningful and considered analysis of the considerable and varied evidence base regarding the Bill. The consultation on the development of the Bill and the parallel development of rules by the Department of Home Affairs while the Committee inquiry was

underway led to inconsistent engagement from industry with the Committee process, as well as an evolving and shifting evidence base during the course of the inquiry. The ongoing considerable workload of the Committee constrained its ability to engage with all interested parties, and when paired with the effect of COVID-19 lockdowns and restricted Parliamentary processes, the Committee has been unable to resolve all the disputes put before it.

The Committee is also conscious that there is limited time left in the Parliamentary sitting calendar in 2021 and that sittings have previously been disrupted due to local outbreaks and lockdowns. Given this small and rapidly diminishing window of opportunity to legislate, it is necessary to prioritise the most urgent elements of the legislation.

These factors have led the Committee to the conclusion that the SOCI Bill should be split to legislate promptly the urgent measures which seek to address the immediate threat, while deferring the remainder of the proposed framework to be revisited and amended in a consultative and collaborative basis with those entities affected, so that industry can work actively with the Government to achieve an agreed way forward for these essential critical infrastructure assets to be protected.

The urgency for response from an escalating threat was stated by the Secretary of the Department of Home Affairs:

> … once the bill achieves royal assent as an act of parliament it allows us to activate certain emergency procedures under the government assistance measures, and it is those measures that, frankly, I would prefer to have on the statute books tonight.[1]

In response to this threat, the Committee recommends that the SOCI Bill be split in two, so that the current Bill can be amended (Bill One) to allow urgent elements of the reforms such as government assistance mechanisms, mandatory notification requirements and related measures to be swiftly legislated. This will ensure that the Government can exercise these vital powers when 'last resort' circumstances arise.

However, passage of only the government assistance mechanisms in Bill One, and not the remaining positive security obligations and other measures, does risk moral hazard where cyber-security for critical infrastructure is regarded as "the government's job" instead of a shared partnership between industry and government.

---

1 Mr Michael Pezzullo AO, Secretary, Department of Home Affairs, *Committee Hansard*, Canberra, 29 July 2021, p. 10.

The Committee therefore recommends that the remaining elements of the SOCI Bill be amended in consultation with industry, and reintroduced in a subsequent Bill (Bill Two) containing the less urgent measures, such as risk management programs and declarations of Systems of National Significance (with accompanying enhanced cyber security obligations). Bill Two can then proceed at a more manageable pace for government and industry and ensure that the Security of Critical Infrastructure framework that Australia needs generates broad stakeholder consensus.

The Committee believes that the elements in Bill Two, following appropriate consultation and amendment where necessary, are essential because they recognise that industry has its own obligations to secure essential services for their customers and the nation.

The Committee is also recommending that Bill Two be referred to the Committee when it is introduced for further review, alongside analysis of the impacts of the more urgent Bill One. This is accompanied by a further statutory review mechanism of the *Security of Critical Infrastructure Act 2018* in the future, to ensure that these considerable legislative reforms are not just a 'set and forget' response to a current threat.

Contents

List of Tables

Abbreviations

ACSC	Australian Cyber Security Centre
AEC	Australian Electoral Commission
APRA	Australian Prudential Regulation Authority
ASD	Australian Signals Directorate
CIC	Critical Infrastructure Centre
IGIS	Inspector-General of Intelligence and Security
IS Act	*Intelligence Services Act 2001*
OAIC	Office of the Australian Information Commissioner
PSOs	Positive security obligations
SOCI Bill	Security Legislation Amendment (Critical Infrastructure) Bill 2020
SoNS	Systems of national significance
Telco Act	*Telecommunications Act 1997*
TIA Act	*Telecommunications (Interception and Access) Act 1979*
TSSR	Telecommunications Sector Security Reforms

Members

Chair

Senator James Paterson (from 04/02/2021)

Mr Andrew Hastie MP (until 22/12/2020)

Deputy Chair

Hon Anthony Byrne MP

Members

Hon Mark Dreyfus QC MP

Mr Julian Leeser MP

Mr Tim Wilson MP

Ms Celia Hammond MP (from 03/02/2021)

Dr Anne Aly MP

Senator Amanda Stoker (until 22/12/2020)

Senator the Hon Eric Abetz

Senator Jenny McAllister

Senator the Hon David Fawcett

Senator the Hon Kristina Keneally

Terms of Reference

The Security Legislation Amendment (Critical Infrastructure) Bill 2020 was introduced into the House of Representatives by the Hon Peter Dutton MP, the then Minister for Home Affairs, on 10 December 2020 and was referred to the Committee by the Hon Christian Porter MP, the then Attorney-General, on 11 December 2020 for inquiry and report. The Bill proposes amendments to the existing *Security of Critical Infrastructure Act 2018*.

Section 60A of the *Security of Critical Infrastructure Act 2018* requires the Committee to commence a review into the operation, effectiveness and implications of the reforms introduced in the Act by 11 April 2021.

As the Bill referred amends the regime provided for by the existing Act, which would be reviewed as per section 60A, the Attorney-General suggested that the Committee commence the statutory review in conjunction with the Bill review, especially in relation to "the requirement at paragraph 60A(l)(b) noting that the Bill seeks to amend the SOCI Act to capture additional assets as critical infrastructure assets. This requires the Committee to consider the appropriateness of a unified scheme to cover all critical infrastructure assets".

The Committee agreed with this contention, and launched the statutory review of the *Security of Critical Infrastructure Act 2018* in conjunction with the Bill review.

List of Recommendations

Recommendation 1

3.21 The Committee recommends that the Security Legislation Amendment (Critical Infrastructure) Bill 2020 be split in two, so that the urgent elements of the reforms contained within the government assistance measures in proposed Part 3A, with the definitions and meanings of expanded critical infrastructure sectors and assets, and other enabling provisions contained within proposed amendments to Part 1, Part 2B, Part 4, Part 5 and Schedule 2 of the current Bill, be retained, amended in line with the principles outlined in paragraph 3.18 of this report, and legislated in the shortest time possible (Bill One).

Recommendation 2

3.30 The Committee recommends that proposed Part 2B of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 be retained in Bill One, and that Part be amended to:

- extend the requirement under proposed section 30BC for formal written notification to be made by an affected entity within 84 hours if an initial oral notification is given when a critical cyber security incident is having a significant impact on the availability of the critical infrastructure asset the entity is responsible for; and

- that proposed sections 30BC and 30BD be amended to allow for an entity and the relevant Commonwealth body to agree that a written notification is not required for an incident, if upon investigation it is agreed that the incident does not meet the requirement of an incident or does not have the defined impact outcome.

Recommendation 3

3.32 The Committee recommends that the rules to be designed for the purposes of amended Part 2B of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 be developed in consultation with relevant entities and incorporated into explanatory material to Bill One.

Recommendation 4

3.36 The Committee recommends that Bill One include a provision that as soon as practicably after a government assistance measure is directed or requested the Parliamentary Joint Committee on Intelligence and Security be notified in writing about the circumstances, actions, status and parties involved in each measure used relative to any cyber security incident.

Recommendation 5

3.39 The Committee recommends that, subject to the amendments outlined above, the resultant Security Legislation Amendment (Critical Infrastructure) Bill (Bill One) be passed.

Recommendation 6

3.44 The Committee recommends that the Cyber and Infrastructure Security Centre within the Department of Home Affairs, be reformed to additionally provide technical support and advice regarding the functions of Bill One.

Recommendation 7

3.50 The Committee recommends that the remaining non-urgent elements of the current Security Legislation Amendment (Critical Infrastructure) Bill 2020 not recommended for inclusion in Bill One, be deferred and amended into a separate Bill (Bill Two) in line with the principles outlined in paragraph 3.49.

Recommendation 8

3.54 The Committee recommends that Bill Two be amended in consultation with key stakeholders, released for feedback and with further consultation on incorporated amendments based on that feedback, prior to being reintroduced to Parliament.

Once reintroduced, Bill Two should be referred to the Parliamentary Joint Committee on Intelligence and Security for review, with a concurrent review

of the operation to date of the amendments to the *Security of Critical Infrastructure Act 2018* resulting from Bill One.

Recommendation 9

3.57 The Committee recommends that any rules to be designed under Bill Two be co-designed, agreed and finalised to the extent possible before the introduction of that Bill and made available as part of the explanatory material for the Bill.

Recommendation 10

3.63 The Committee recommends that proposed Schedule 2 of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 be amended in accordance with the principles outlined in paragraph 3.62 and included as part of Bill One.

Recommendation 11

3.68 The Committee recommends that subsection 13A(2) of the *Intelligence Services Act 2001* be amended to restrict cooperation or assistance provided by an agency under that Act to agencies or other bodies by regulation outlined in subsection 13A(1) only to the functions and extent authorised by other Commonwealth legislation.

Recommendation 12

3.79 The Committee recommends the Government review the risks to democratic institutions, particularly from foreign originated cyber-threats, with a view to developing the most appropriate mechanism to protect them at Federal, State and local levels.

Recommendation 13

3.85 The Committee recommends the Government review the processes and protocols for classified briefings for the Opposition during caretaker periods in response to serious cyber-incidents, and consider the best practice principles for any public announcement about those incidents.

Recommendation 14

4.16 The Committee recommends that the Bill One include a provision that the Parliamentary Joint Committee on Intelligence and Security may conduct a

review of the operation, effectiveness and implications of the reformed security of critical infrastructure legislative framework contained within the *Security of Critical Infrastructure Act 2018* not less than three years from when that Bill receives Royal Assent.

1. Introduction

The Bill and referral

1.1 The Security Legislation Amendment (Critical Infrastructure) Bill 2020 (the SOCI Bill) was introduced to the House of Representatives by the Hon Peter Dutton MP, then Minister for Home Affairs on 10 December 2020, the final Parliamentary sitting day of 2020.

1.2 In his second reading speech Minister Dutton outlined the rationale for the SOCI Bill:

> Critical infrastructure underpins the delivery of goods and services that are essential to the Australian way of life, our nation's wealth and prosperity, and national security.
>
> While Australia has not suffered a catastrophic attack on our critical infrastructure, we are not immune.
>
> Australia is facing increasing cybersecurity threats to essential services, businesses and all levels of government. In the past two years we have seen cyberattacks on federal parliamentary networks, logistics, the medical sector and universities, just to mention a few.
>
> Internationally, we have seen cyberattacks on critical infrastructure, including water services and airports.
>
> COVID-19 has also strained the ability of critical infrastructure to deliver essential services. These disruptions show how quickly events can cause widespread physical, financial and indeed psychological damage.
>
> While owners and operators of critical infrastructure are best placed to deal with such threats, it takes a team effort to bring about positive change. That is why the ongoing security and resilience of critical infrastructure must be a

> shared responsibility, not only by all governments and the owners and operators of the infrastructure but indeed by all Australians. The cost of inaction is far too great to ignore.[1]

1.3 The SOCI Bill's Explanatory Memorandum summarises the intended reforms as:

> …an enhanced regulatory framework, building on existing requirements under the SOCI Act. The Security Legislation Amendment (Critical Infrastructure) Bill 2020 gives effect to this framework by introducing:
>
> - additional positive security obligations for critical infrastructure assets, including a risk management program, to be delivered through sector-specific requirements, and mandatory cyber incident reporting;
> - enhanced cyber security obligations for those assets most important to the nation, described as systems of national significance; and
> - government assistance to relevant entities for critical infrastructure sector assets in response to significant cyber attacks that impact on Australia's critical infrastructure assets.[2]

1.4 On 11 December 2020 the Hon Christian Porter MP, then Attorney-General, wrote to the Committee to refer the provisions of the SOCI Bill to the Committee for inquiry and report pursuant to subparagraph 29(b)(ia) of the *Intelligence Services Act 2001* (the IS Act), noting the relevance to this provision as the SOCI Bill engages the Australian Signals Directorate as the technical authority.[3]

1.5 As a result of a recommendation in the Committee's Advisory Report on the Security of Critical Infrastructure Bill 2017, section 60A of the *Security of Critical Infrastructure Act 2018* (the Act) requires the Committee to commence a review into the operation, effectiveness and implications of the reforms introduced in the Act by 11 April 2021.

1.6 As the proposed SOCI Bill amends the regime provided for by the Act, which would be reviewed as per section 60A, the Attorney-General suggested that the Committee commence the statutory review in conjunction

---

1 The Hon Peter Dutton MP, Minister for Home Affairs, *House of Representatives Hansard*, 10 December 2020, pp. 11262-11263.

2 Explanatory Memorandum, p. [2].

3 The Attorney-General's referral letter is available at https://www.aph.gov.au/DocumentStore.ashx?id=fdef8237-d91e-415e-aee3-9d9043d2131f

with the SOCI Bill review, especially in relation to "the requirement at paragraph 60A(l)(b) noting that the Bill seeks to amend the SOCI Act to capture additional assets as critical infrastructure assets. This requires the Committee to consider the appropriateness of a unified scheme to cover all critical infrastructure assets".

Conduct of the inquiry

1.7 The Committee resolved to undertake an inquiry into the SOCI Bill, agreed with the Attorney-General's suggestion, and launched the Bill inquiry and statutory review of the *Security of Critical Infrastructure Act 2018* as a joint inquiry on 21 December 2020, with details uploaded to the Committee's website at www.aph.gov.au/pjcis. Submissions were invited and requested by 12 February 2021 (aligning with submission requests for two other Bill inquiries launched by the Committee in December 2020).

1.8 The Committee received 88 submissions (including three confidential submissions), 66 supplementary submissions, and four attachments (three confidential) over the course of the inquiry, made up of extra submissions, answers to Questions on Notice, opening statements from panel public hearings, and other material provided by submitters or upon request. A list of submissions can be found at Appendix A.

1.9 The Committee held public hearings on 11 June 2021 and 8, 9 and 29 July 2021. A list of witnesses appearing at the public hearings can be found at Appendix B.

1.10 The Committee has also received private (classified) briefings throughout the 46th Parliament regarding the threat environment and increasing hazard of cyber security to critical infrastructure within Australia.

1.11 Copies of submissions, transcripts of proceedings from public hearings[4], and links to the SOCI Bill and Explanatory Memorandum can be accessed from the Committee's webpage.

Report structure

1.12 The report consists of four chapters:

[4] Hansard transcripts referenced throughout this report are taken from Proof transcripts. Accuracy of verbatim evidence is not assured, however Official transcripts incorporating corrections from witnesses will be available on the Committee's website in due course.

- This chapter sets out the context and conduct of the inquiry and the concurrent status of this inquiry with other Committee processes;
- Chapter 2 provides an outline of the SOCI Bill, the threat that is to be countered by the proposed framework, the main themes of evidence received by the Committee, with a focus on the key points of contention, as well as a summary of the challenges faced in the conduct of the inquiry;
- Chapter 3 outlines the Committee's identified priority for the SOCI Bill's intended impact, as well as recommendations for a way forward to address the cyber security threat to Australia's critical infrastructure; and
- Chapter 4 briefly identifies proposed Committee action regarding the statutory review of the Act and the related statutory review of Part 14 of the *Telecommunications Act 1997* – Telecommunications Sector Security Reforms (the TSSR Review).

Concurrent reviews

1.13 As outlined above, the Committee agreed to commence the statutory review required under section 60A of the Act at the same time as adopting the Bill review.

1.14 The statutory review requirements in section 60A were set based on recommendation 9 of the Committee's *Advisory Report on the Security of Critical Infrastructure Bill 2017*.[5] Those requirements are:

> **60A Review of this Act**
>
> (1) The Parliamentary Joint Committee on Intelligence and Security must:
>
> (a) review the operation, effectiveness and implications of this Act; and
>
> (b) without limiting paragraph (a), consider whether it would be appropriate to have a unified scheme that covers all infrastructure assets (including telecommunication assets) that are critical to:
>
> (i) the social or economic stability of Australia or its people; or
>
> (ii) the defence of Australia; or

[5] Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Security of Critical Infrastructure Bill 2017*, 2018, p. 53.

(iii) national security; and

(c) review the circumstances in which any declarations have been made under Part 6 of this Act (declarations of assets by the Minister); and

(d) report the Committee's comments and recommendations to each House of the Parliament.

1.15 These requirements were set in recommendation by the Committee to allow for the review of the Act and requisite assessment of whether the contentions made by the Australian Government regarding the establishment of the Act were appropriate.

1.16 The focus on the above aspects of the operation of the Act were in response to industry concerns raised about a lack of clarity in that Bill regarding Ministerial directions power, definitions and their scope, and the potential effect of Commonwealth directions on State owned critical infrastructure entities.[6] Similar concerns have been mirrored regarding the Bill relevant to this report, which will be discussed further in Chapter 2.

1.17 In consideration of the statutory review requirements, as the Committee received submissions, most industry representatives expressed little to no view on the operation of the existing Act, focusing on the expansions provided for in the SOCI Bill instead. Similarly the Department of Home Affairs (the Department), the regulator for the Act and the proposed expanded regime in the SOCI Bill, only provided five pages out of its 45 page primary submission regarding the operation of the Act to the date the SOCI Bill was referred.[7]

1.18 This primary focus on the SOCI Bill alone has presented a challenge to the Committee in conducting the concurrent statutory review. This challenge was compounded by the fact that the Bill under review amends the Act to be reviewed, making concurrent analysis problematic.

1.19 This challenge and the result is commented on further in Chapter 4.

---

6 Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Security of Critical Infrastructure Bill 2017*, 2018, pp. 51-53.

7 Department of Home Affairs, *Submission 59*, pp. 7-11.

Review of Part 14 of the Telecommunications Act 1997 – Telecommunications Sector Security Reforms

1.20 The Committee is conducting the TSSR review contemporaneously with this Bill review. While the TSSR was established to provide a regulatory framework to manage the national security risks of espionage, sabotage and foreign interference to Australia's telecommunications networks and facilities and resides within the *Telecommunications Act 1997* (the Telco Act), the SOCI Bill under review proposes to potentially subsume the regulation of telecommunications for the purposes of many of these risks.

1.21 Much like the statutory review of the Act, a majority of the evidence received by the Committee in submissions and public hearing testimony was dedicated to the proposed changes to the sector from the SOCI Bill, somewhat hampering the Committee's ability to conduct the related, yet discrete, review required under the Telco Act.

1.22 More commentary on this is provided for in Chapter 4 of this report.

2. The Bill and evidence themes

The Bill

2.1 The following is an extract of the Bill outline from the Explanatory Memorandum, providing the rationale for the SOCI Bill and a brief explanation of the reforms contained within.

> The Australian Government is committed to protecting the essential services all Australians rely on by uplifting the security and resilience of our critical infrastructure. As the threats and risks to Australia's critical infrastructure evolve in a post-COVID world, so too must our approach to ensuring the ongoing security and resilience of these assets and the essential services they deliver.
>
> Critical infrastructure is increasingly interconnected and interdependent, delivering efficiencies and economic benefits to operations. However, connectivity without proper safeguards creates vulnerabilities that can deliberately or inadvertently cause disruption and result in cascading consequences across our economy, security and sovereignty.
>
> Threats ranging from natural hazards (including weather events) to human induced threats (including interference, cyber attacks, espionage, chemical or oil spills, and trusted insiders) all have the potential to significantly disrupt critical infrastructure. Recent incidents such as compromises of the Australian parliamentary network, university networks and key corporate entities, and the impacts of COVID-19 illustrate that threats to the operation of Australia's critical infrastructure assets continue to be significant. Further, the interconnected nature of our critical infrastructure means that compromise of one essential function can have a domino effect that degrades or disrupts others.

The consequences of a prolonged and widespread failure in the energy sector, for example, could be catastrophic to our economy, security and sovereignty, as well as the Australian way of life, causing:

- shortages or destruction of essential medical supplies;
- instability in the supply of food and groceries;
- impacts to water supply and sanitation;
- impacts to telecommunications networks that are dependent on electricity;
- the inability of Australians to communicate easily with family and loved ones;
- disruptions to transport, traffic management systems and fuel;
- reduced services or shutdown of the banking, finance and retail sectors; and
- the inability for businesses and governments to function.

While Australia has not suffered a catastrophic attack on critical infrastructure, we are not immune:

- over the last two years, we have seen several cyber attacks in Australia that have targeted the Federal Parliamentary Network;
- malicious actors have taken advantage of the pressures COVID-19 has put on the health sector by launching cyber attacks on health organisations and medical research facilities; and
- key supply chain businesses transporting groceries and medical supplies have also been targeted.

Accordingly, Government will introduce an enhanced regulatory framework, building on existing requirements under the SOCI Act. The Security Legislation Amendment (Critical Infrastructure) Bill 2020 gives effect to this framework by introducing:

- additional positive security obligations for critical infrastructure assets, including a risk management program, to be delivered through sector-specific requirements, and mandatory cyber incident reporting;
- enhanced cyber security obligations for those assets most important to the nation, described as systems of national significance; and
- government assistance to relevant entities for critical infrastructure sector assets in response to significant cyber attacks that impact on Australia's critical infrastructure assets.

These changes will be underpinned by enhancements to Government's existing education, communication and engagement activities, under a

refreshed Critical Infrastructure Resilience Strategy. This will include a range of activities that will improve our collective understanding of risk within and across sectors.

The enhanced framework will uplift security and resilience in all critical infrastructure sectors. When combined with better identification and sharing of threats, this framework will ensure that Australia's critical infrastructure assets are more resilient and secure. Government will work in partnership with responsible entities of critical infrastructure assets to ensure the new requirements build on and do not duplicate existing regulatory frameworks.

This framework will apply to owners and operators of critical infrastructure regardless of ownership arrangements. This creates an even playing field for owners and operators of critical infrastructure and maintains Australia's existing open investment settings, ensuring that businesses who apply security measures are not at a commercial disadvantage.

The Australian Government's Critical Infrastructure Resilience Strategy currently defines critical infrastructure as:

'those physical facilities, supply chains, information technologies and communication networks, which if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security.'

In the context of this, the SOCI Act currently places regulatory obligations on specific entities in the electricity, gas, water and maritime ports sectors. However, as the security landscape evolves, so must our approach to managing risk across all critical infrastructure sectors.

As such, the amendments in this Bill will enhance the obligations in the SOCI Act, and expand its coverage to the following sectors: communications; financial services and markets; data storage and processing; defence industry; higher education and research; energy; food and grocery; health care and medical; space technology; transport; and water and sewerage.

The reforms

The Commonwealth needs to establish a clear, effective, consistent and proportionate approach to ensuring the resilience of Australia's critical infrastructure. The amendments to the SOCI Act will drive the uplift of the security and resilience of Australia's critical infrastructure.

The Security Legislation Amendment (Critical Infrastructure) Bill 2020 (the Bill) will introduce an all-hazards positive security obligation for a range of critical infrastructure assets across critical sectors. This ensures industry is taking the appropriate steps to manage the security and resilience of their assets. The obligations to be included in the Act in relation to a critical infrastructure risk management program will be supported by specific requirements which will be prescribed in rules, which will be co-designed between industry and government.

The Bill also recognises those assets that are the most critical to the security, economy and sovereignty of Australia. These 'systems of national significance' will bear additional cyber obligations recognising the cyber threat environment we currently face.

Finally, while these measures are designed to ensure we do not suffer a catastrophic cyber attack, the Bill will ensure Government has the necessary powers to provide direct assistance to industry in the event of a serious cyber security incident.

Positive Security Obligations

The additional positive security obligations will build on the existing obligations in the SOCI Act to embed preparation, prevention and mitigation activities into the business as usual operating of critical infrastructure assets, ensuring that the resilience of essential services is strengthened. It will also provide greater situational awareness of threats to critical infrastructure assets.

The positive security obligations involve three aspects:

- adopting and maintaining an all-hazards critical infrastructure risk management program;
- mandatory reporting of serious cyber security incidents to the Australian Signals Directorate (ACSC); and
- where required, providing ownership and operational information to the Register of Critical Infrastructure Assets.

Importantly, each aspect of the positive security obligations will only apply once a rule is made in relation to that aspect for a critical infrastructure asset or class of critical infrastructure assets. The rules will prescribe which aspects are 'switched on' for a critical infrastructure asset or class of critical infrastructure assets.

The critical infrastructure risk management program will require responsible entities of specified critical infrastructure assets to manage and mitigate risks.

Responsible entities of critical infrastructure assets will be required to take an all-hazards approach when identifying and understanding those risks – both natural and human induced hazards.

Responsible entities of specified critical infrastructure assets will be required to report cyber security incidents to the relevant Commonwealth body. Collecting this information will support the development of an aggregated threat picture to inform both proactive and reactive cyber response options – from providing immediate assistance to working with industry to uplift broader security standards.

Part 2 of the current SOCI Act requires assets covered by the Act to provide ownership and operational information to the Secretary of Home Affairs for the Register of Critical Infrastructure Assets (the Register). The Bill will extend this requirement to the expanded class of critical infrastructure assets where appropriate to develop and maintain a comprehensive picture of national security risks, and apply mitigations where necessary.

Enhanced Cyber Security Obligations for systems of national significance

The Enhanced Cyber Security Obligations in the Bill will support a bespoke, outcomes-focused partnership between Government and Australia's 'systems of national significance.' These are a significantly smaller subset of critical infrastructure assets that are crucial to the nation, by virtue of their interdependencies across sectors and consequences of cascading disruption to other critical infrastructure assets and sectors.

Under the Enhanced Cyber Security Obligations, the Secretary of Home Affairs may require the responsible entity for a system of national significance to undertake one or more prescribed cyber security activities. These include the development of cyber security incident response plans, cyber security exercises to build cyber preparedness, vulnerability assessments to identify vulnerabilities for remediation, and the provision of system information to build Australia's situational awareness.

The Enhanced Cyber Security Obligations will support the sharing of near-real time threat information to provide industry with a more mature understanding of emerging cyber security threats, and the capability to reduce the risks of a significant cyber attack against Australia's most critical assets.

Government Assistance

This Bill introduces a Government Assistance regime to respond to serious cyber security incidents that applies to all critical infrastructure sector assets. Government recognises that industry should and in most cases, will respond

to the vast majority of cyber security incidents, with the support of Government where necessary. However, Government maintains ultimate responsibility for protecting Australia's national interests. As a last resort, the Bill provides for Government assistance to protect assets immediately prior, during or following a significant cyber attack.

2.2 More specifically, Schedule 1, Part 1 of the SOCI Bill is separated into:

- proposed amendments to the *Administrative Decisions (Judicial Review) Act 1977* and *AusCheck Act 2007* to enable proposed review exclusions and background checks;
- proposed amendments made to existing Part 2 of the Act for expansion of the information required for the Register of Critical Infrastructure Assets;
- a new proposed Part 2A to introduce risk management programs;
- a new proposed Part 2B to introduce mandatory cyber incident reporting;
- a new proposed Part 2C outlining enhanced cyber security obligations of entities set by declarations from the Secretary of the Department (the Secretary) as systems of national significance (SoNS);
- a new proposed Part 3A to introduce powers of government assistance (including intervention, information gathering and action directions); and
- a new proposed Part 6A outlining the mechanisms for SoNS declarations.

2.3 Schedule 1, Part 2 of the SOCI Bill defines application provisions.

2.4 Schedule 1, Parts 3 and 4 of the SOCI Bill enables updates of terminology regarding the impacts of the *Federal Circuit and Family Court of Australia Act 2021* and *National Emergency Declaration Act 2020*.

2.5 Schedule 2 of the SOCI Bill proposes amendments to the *Criminal Code Act 1995* to limit liability for ASD to perform certain acts under the Bill that would otherwise contravene or be prohibited by Commonwealth or State and Territory laws regarding computer-related activities.

2.6 The majority of the detail regarding specific requirements of critical infrastructure entities under regulation is identified to be designed and outlined in 'rules' under the SOCI Bill, identified as disallowable legislative instruments under the Explanatory Memorandum, but not under the Bill itself.

2.7 The Committee will not be including further commentary regarding the Bill's substance in this report, except at the sections relevant to commentary regarding impact of proposed elements of the SOCI Bill and any subsequent recommendations.

The threat to be countered

2.8 The main rationale for the SOCI Bill and the expansion of the government's critical infrastructure security focus is outlined in the Explanatory Memorandum extract above. The Department and ASD expanded on these threats and their impact in their primary submissions.[1]

2.9 The expanding threat of cyber security vulnerability and malicious cyber activity has become increasingly evident in recent years. Australia has enjoyed relative security in this regard, but recent years have highlighted that both government and the private sector are not immune. The incidence of cyber attacks, ransomware and exploitation of system vulnerabilities is accelerating at an ever-increasing pace.

2.10 High profile cyber security incidents affecting government departments, including Parliamentary networks[2], major logistics and transport companies like Toll Group[3], or media companies like the Nine Network[4], bring mainstream attention to the ongoing and persistent attacks that Australian companies and networks face every day.

2.11 These attacks are just the most public face of the threat, with the Australian Cyber Security Centre (ACSC) reporting 2,266 reported incidents in 2019-20, with just over a third of those incidents coming from critical infrastructure companies and assets.[5]

---

1 ASD, *Submission 9*, pp. 2-3; Department of Home Affairs, *Submission 59*, pp. 12-17.

2 ASD, *Submission 9*, p. 2.

3 Australian Financial Review, *Hacked again: Toll Group systems hit by fresh ransomware attack*, 5 May 2020, accessed 19 August 2021, https://www.afr.com/technology/hacked-again-toll-group-systems-hit-by-fresh-ransomware-attack-20200505-p54q19

4 9 News, *Nine Network under attack by cyber hackers, threatening news services nationwide*, 29 March 2021, accessed 19 August 2021, https://www.9news.com.au/national/nine-network-hit-by-cyber-attack-threatening-news-services-nationwide/c653fe12-a5c4-4da8-9a33-b902f1325eed

5 ASD, *Submission 9*, pp. 2-3.

2.12 When outlining these threats and the increasing challenge of preparing, hardening and countering assets, Mr Michael Pezzullo AO, Secretary of the Department of Home Affairs, stated:

> Cyber attacks will soon reach global pandemic proportions. This has been building for about five years but has accelerated over the course of the COVID pandemic. The minister has directed that we build on the Cyber Security Strategy launched in 2020 with an increased focus on protecting critical infrastructure—that's what brings us before you today—cybercrime operations, counter-ransomware, along with intensified engagement with states, territories, industry and the general public.
>
> Basic cyber security protections will always help, but malicious actors, such as cybercriminals, state sponsored actors and state actors themselves will defeat the best defences that firms, families and individuals can buy. We have to do what we can, of course, to defend our own networks and devices against known vulnerabilities. However, just as we do not rely on home security alarms and door locks to deal with serious and organised crime, we cannot leave firms, families and individuals on the field on their own.
>
> …
>
> We have to be prepared to conduct offensive operations in the havens of cybercriminals. Cyber is not immaterial. It is material. It is reliant on infrastructure, hardware, coding spaces for the coders and physical staging points. These havens can be mapped and targeted. Nations such as Australia have an asymmetric advantage because unlike in terms of military strength—where great powers have a symmetric advantage—should we have the will, the strategies, the authorities and the means, we can gain asymmetric advantages including when we go on the offensive. It's already the case that policing and intelligence agencies as well as military cyber forces within authorities are striking at the infrastructure of these malicious actors in their havens, where regrettably some states either turn a blind eye to their activities or actively enable and sponsor them. Regrettably, state protection emboldens these malicious actors.
>
> One model to tackle this challenge is the counterterrorism model that was put in place after 9/11 to deal with al-Qaeda. Another model that I would suggest to this committee, that is worth reflecting on as you consider this bill and consider your report, is the campaign that was mounted in the 17th, 18th and then in the beginning of the 19th century to clear the world's oceans of pirates, including the pirates of the Caribbean who were defeated by Her Majesty's warships of the royal navy in concert with bringing law to a lawless ocean.

> This is a problem with which we can deal, just as Britain overcame piracy, but we need the tools to do so including the requisite legal authorities.[6]

2.13 *Australia's Cyber Security Strategy 2020* foreshadowed and outlined this response when it was delivered in August 2020:

> The Australian Government must be ready to act in the national interest when its unique capabilities are needed, especially in emergency situations.
>
> In consultation with critical infrastructure owners and operators, the Australian Government will develop new powers proportionate to the consequences of a sophisticated and catastrophic cyber attack, accompanied by appropriate safeguards and oversight mechanisms.
>
> These powers will ensure the Australian Government can actively defend networks and help the private sector recover in the event of a cyber attack.
>
> The nature of this assistance will depend on the circumstances, but could include expert advice, direct assistance or the use of classified tools. This will reduce the potential down-time of essential services and the impact of cyber attacks on Australians.[7]

2.14 Evidence was received from a panel of experts at the public hearing on 9 July 2021, highlighting the agreed state of a shift in the cyber threat environment. This shift was summarised by Mr Chris Krebs:

> …there have been three strategic shifts over the last several years in the threat actor landscape. First, as you already mentioned, was ransomware and criminal actors. I don't want to gloss over the fact that it is important that the public—the American public, the Australian public and the public elsewhere—finally recognise the true disruptive nature of cyber security in general, after decades of intelligence based actions that have been, by design, subtle and covert. Now, when we have these brazen, in-your-face, disruptive attacks—particularly here in the US, but also in Australia—when your hamburgers and hotdogs have been taken off the shelves, I think that finally brings it home and makes it really resonate.
>
> I think the second strategic shift that we've seen was probably over the last two to three years, where, rather than go after their primary targets through the front door, the intelligence apparatus of our adversaries—traditionally, from the US perspective at least, we call that Russia, China, Iran and North

---

6 Mr Michael Pezzullo AO, Secretary, Department of Home Affairs, *Committee Hansard*, Canberra, 11 June 2021, pp. 25-26.

7 Commonwealth of Australia, *Australia's Cyber Security Strategy 2020*, p. 22.

> Korea, but obviously there are others—have sought to effectively use the global ICT ecosystem, the systems we use on a daily basis, as a real-time collection apparatus. When you think about SolarWinds, that's how I would be thinking about it: taking advantage of the IT systems that we use and deploy without fully appreciating the risk and the elevated access these systems have.
>
> The third and final strategic shift that I'd suggest we really prioritise is a shifting to functional disruptions and moving away from purely reconnaissance and intelligence collection. As great power conflict increases, particularly in the case of Russia or China, we will see colder or warmer activity. What we may see is precursor operations that disable infrastructure to prevent the opposing power from being able to project power.[8]

2.15 This strategic shift and the rise of cyber-enabled crime and security threats has not been countered evenly by entities:

> …there's an uneven investment in cyber security. There are companies out there, if you look to the JP Morgans or Bank of Americas, that size and sophistication of entities, that are spending almost $1 billion a year on cyber security programs, which is clearly a significant investment for a company of any size. But it's absolutely true that it's not consistent across industry. I think at least part of the objectives of the bill should be ensuring that everybody is levelling up but doing so without inhibiting the good work that many companies are doing already.[9]

2.16 In response to this shift and the uneven response to it, the SOCI Bill's rationale states that there is a requirement for the measures outlined, but that time for a measured response is limited, if not already past, as identified by the Secretary:

> We're already past time. The clock is ticking. The possibility of us waking up tomorrow and being in the grip of such an attack was already last year or the year before. The urgency of this legislation, frankly, is I would think self-evident, particularly for those who have seen the intelligence that is relevant here…two parts: each sector will be different; I don't think there will ever be a

---

8 Mr Christopher Krebs, Partner, Krebs Stamos Group, *Committee Hansard*, Canberra, 9 July 2021, pp. 5-6.

9 Mr Alexander Botting, Director, International Policy, Coalition to Reduce Cyber Risk, *Committee Hansard*, Canberra, 9 July 2021, p. 6.

> clean start line. Secondly, the imperative is so overwhelming that we are probably past time.[10]

2.17 The imperative for the reforms was not contested in evidence to the inquiry, but significant concerns about the process to develop government's response was presented to the Committee, as outlined further below.

Committee comment

2.18 The Committee is highly aware of the threat that Australia faces from cyber-enabled national security and critical infrastructure threats. A large proportion of the national security legislation that the Committee has considered in this and previous Parliaments has been in response to rising information technology risks and cyber-enabled threats; however these powers have been to enable government and law enforcement and intelligence agencies to respond when that threat can be countered directly.

2.19 The Committee recognises that the proposed critical infrastructure framework in the SOCI Bill is to enable the government to assist critical infrastructure assets to counter and respond to these threats in the best way possible, preferably in a cooperative fashion, but also in a 'step-in' fashion if required. However, the time window in which that response and assistance can be delivered is closing rapidly, as the threat increases.

2.20 This need for timely action and the appropriate response within the proposed framework and time available, but without uncertain regulatory cost, is outlined by the Committee in Chapter 3.

Evidence received

2.21 As mentioned in Chapter 1, the Committee received substantial evidence in submissions to the inquiry. These submissions were received from companies that will be affected directly by the proposed framework in the SOCI Bill, representative organisations advocating for member companies or on the sector impacts more generally, cyber security or technology companies or consultants, trade unions, State governments, Commonwealth agencies affected by the SOCI Bill, and legal peak bodies.[11]

---

10 Mr Michael Pezzullo AO, Secretary, Department of Home Affairs, *Committee Hansard*, Canberra, 29 July 2021, p. 6.

11 All primary and supplementary submissions, incorporating answers to questions on notice or further material requested from witnesses, to the Bill review are available from the inquiry website at

2.22 This wide-ranging evidence base presented diverse and varied opinions on the intent of the SOCI Bill, as well as the prospective regulatory and business impacts that the SOCI Bill could present to the entities affected. Much of the evidence focused on the current business practices of those companies, the cyber security practices and systems in place, as well as any existing regulatory systems and standards implemented and applied.

2.23 This variation in evidence, specific to the eleven critical infrastructure sectors was useful evidence to the Committee's considerations of the potential impact of the SOCI Bill. However, the commentary provided below has had to be restricted to that evidence specific to the need for reform, the broad impact of the SOCI Bill, or common themes of evidence regarding Bill development or regulatory scope.

2.24 The Committee received numerous submissions providing technical evidence regarding cyber security trends, threats or observations of weakness regarding particular industry sectors. These submissions were useful to consideration of the overall threat environment and landscape that the SOCI Bill is attempting to address.

Committee comment

2.25 The Committee thanks all submitters and witnesses that have provided invaluable evidence and insight into the potential impact of the SOCI Bill and the business environment that the reforms propose to address or ameliorate the cyber security threat to. Critical infrastructure assets are vital to the security of our nation and the provision of essential services to its citizens.

2.26 Due to the wide impact of the SOCI Bill, the range of evidence received and the unknown nature of the impact of certain elements of the Bill, the Committee cannot acknowledge or comment on all concerns, recommendations or suggestions made to it. Likewise, the challenges that the Committee continued to face with the conduct of the review, as well as the increasing cyber security threat that the SOCI Bill is intended to address, has meant that the Committee is delivering a shorter thematic report for this review, acknowledging the major shared elements of evidence between submitters and witnesses, while addressing the identified threat to be countered.

---

https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/SOCI/Submissions

2.27 This commentary is below and in the following Chapters.

Themes of evidence received

2.28 The evidence received on the rationale for, and the development of the Bill, as well as the evidence regarding the SOCI Bill itself and its potential regulatory impact is summarised into major themes below.

2.29 This report will not be identifying every submitter or witness that provided information regarding a theme, rather identifying what the theme is with any pertinent points identifying the core of a theme or concern or any particularly relevant evidence.

Consultation on discussion paper and exposure draft

2.30 As mentioned in Chapter 1, the SOCI Bill was developed and introduced to Parliament after consultation processes on a discussion paper and an exposure draft of the Bill.

2.31 These consultation processes were intended to guide the development of the framework proposed in the SOCI Bill, essentially being the first step in the co-design process at the foundation of the regulation that the SOCI Bill proposes to introduce.

2.32 However, the Committee received extensive evidence in submissions and at public hearings that many companies, industry bodies or stakeholders did not feel like their input or feedback had been actioned or acknowledged.

2.33 Many stakeholders also stated there was little promotion of the process, given how wide the impact of the SOCI Bill would be. Medicines Australia stated:

> I don't feel that there was very strong pull action. It was very much: engage if you're interested. Many of the members of Medicines Australia were not aware of the consultation process at all. We felt that there was not enough information on which to provide a really comprehensive submission.[12]

2.34 Acknowledging that not all stakeholders will have been actively engaged with in development, other observations were made that consultation regarding development of the Bill itself was rapid and did not address many of the concerns raised, especially regarding potential duplication of regulation or what rules would be set for each industry sector:

---

12 Ms Elizabeth De Somer, Chief Executive Officer, Medicines Australia, *Committee Hansard*, Canberra, 9 July 2021, p. 57.

> …the consultation process, as people have outlined, has outlined intent, which we understand, but the lack of detail generates lots of questions at our end. Part of consultation is getting feedback on questions and understanding where you can take it, and having that two-way conversation. I don't believe that has really happened. We've had 129 submissions to Home Affairs, and within two weeks we've had a piece of legislation put forward and we're still no clearer on the level of detail we need to understand what level of duplication we'll be dealing with relative to the existing legislation that we work with…[13]

2.35 A number of witnesses at public hearings highlighted that consultation on draft industry rules had improved since initial concerns regarding the Bill's development were made in initial submissions, but the overall hesitancy of industry remained due to the fact that the detail regarding the impact of the Positive Security Obligations (PSOs) within the SOCI Bill are yet to be defined and codified in delegated legislation.

2.36 More commentary on the impact of rules is made later in this Chapter.

Response from the Department to legislative concerns

2.37 As part of the evidence gathering process for this review, the Committee requested that the Department respond to the numerous recommendations raised regarding the SOCI Bill from stakeholders such as the Law Council of Australia, Business Council of Australia, Office of the Australian Information Commissioner (OAIC), Inspector-General of Intelligence and Security (IGIS) and the Commonwealth Ombudsman. Many of these stakeholders raised issues with the Committee regarding the role that their agencies or offices would play within the proposed framework of the SOCI Bill.

2.38 This request was made to allow the Department to consider the merit of the recommendations, many of which had been identified by submitters in the exposure draft consultation process (and not addressed in the resultant Bill), and respond with potential improvements to the Bill taking into account these recommendations, alongside the substantial other evidence base the Committee received.

2.39 In response, the Department provided a supplementary submission (No. 59.1), outlining:

---

[13] Mr Richard Vincent, Chair, National Pharmaceutical Services Association, *Committee Hansard*, Canberra, 9 July 2021, p. 59.

- For the 40 recommendations made by the Law Council of Australia – not accepting 36 of the recommendations and noting the other four without proposing amendment;
- Noting both concerns from the IGIS, with acknowledged amendment to the IS Act being required to bind ASD assistance to the Department for the purposes of an amended version of the Act;
- Noting that OAIC concerns are to be addressed in other proposed legislation or through ongoing consultation; and
- Not supporting any of the 13 proposed legislative changes from the Western Australia Department of Premier and Cabinet.[14]

2.40 While the Department provided reasons of varying complexity for not supporting or accepting the proposed amendments or concerns of submitters, the Committee was not substantially aided by the response in understanding what the impact, if any, of the recommendations would have on the Bill as proposed.

Introduction of the Bill – timing and indicated timelines

2.41 As outlined earlier in this report, the SOCI Bill was introduced on the final sitting day of 2020, and the subsequent request for submissions period for the review spanned Christmas and the New Year period, hampering the efforts of submitters and the Committee to gather initial evidence in a timely manner.

2.42 The then Attorney-General requested that the Bill review be completed by the end of the Autumn sittings which, as outlined in Chapter 1, was not a realistic timeframe. This requested timeframe also aligned with an implementation timetable set out in the Regulatory Impact Statement at Attachment A of the Explanatory Memorandum.[15]

2.43 This timeline stated an expectation that while co-design of rules and economic modelling and guidance would commence in January 2021 and be ongoing, that education and engagement would take place from January to July 2021, with the commencement of the measures in the Bill to apply from 1 July 2021, and enforcement of PSOs to commence on 1 January 2022.

2.44 This timeline raised concerns with submitters, especially in relation to the design of rules, the unknown nature of the impact of that regulatory element of the SOCI Bill's framework, as well as potential enforcement and penalties.

---

14 Department of Home Affairs, *Submission 59.1*.

15 Explanatory Memorandum, pp. 293-294.

2.45 The Communications Alliance expressed the shared sentiment from a number of submitters:

> Given the importance of the sector-specific rules for the success of the entire framework we would believe that it would be wise if the committee advise parliament—or basically push the pause button and create the sector-specific rules first, or at least a substantial part of it and a substantial degree of detail first, before continuing to progress the bill.[16]

2.46 The stated timeline in the Explanatory Memorandum has not been met, and the evidence provided to the Committee indicates that when draft rules have been provided, industry and asset sectors are not ready to accept the indications that rules will address all concerns expressed regarding the Bill.

Sector definition breadth

2.47 In order for the SOCI Bill to apply to relevant industry and asset sectors, those critical infrastructure sectors need to be defined and the assets contained within defined and identified, so the proposed regulations and powers from the Bill can apply accordingly.

2.48 Proposed section 8D of the Bill identifies the relevant sectors and each asset related to those sectors and the responsible entities (that aren't already defined within the Act currently) are defined in proposed amendments to section 5 or proposed sections 12A-12L of the Bill.

2.49 Some of these definitions are necessarily very detailed (see the definition of a critical financial market infrastructure asset in proposed section 12D as an example), and others are very brief and general (see the definition of a critical education asset in proposed amendments to section 5 for example).

2.50 This specificity or generality is accompanied by the vacuum of detail regarding some assets and how they are, or will be, identified in the rules to be set outside of the SOCI Bill (see the definitions of a critical liquid fuel asset in proposed section 12A or a critical freight infrastructure asset at proposed section 12B as examples). These definitions describe the conceptual application of an asset, but leave attribution of specific assets to the rules to be defined in delegated legislation.

2.51 Similarly some definitions capture all assets within a broad sector, such as the definition of a critical data storage or processing asset in proposed

---

16 Ms Christiane Gillespie-Jones, Director, Program Management, Communications Alliance, *Committee Hansard*, Canberra, 9 July 2021, p. 59.

section 12F, but then identify that some specific assets may *not* be an asset as defined, if precluded in the rules. This particular asset definition also does not seemingly recognise potential extraterritorial impact of the broad coverage of this definition, as affected providers may operate within Australia on relevant data held within Australia, but may hold part of that data offshore, or shift it offshore or have primary operations (including data centre assets) in other countries. This is in contrast to many of the other assets that relate to physical assets bound to Australian territory and operation within the country.

2.52 The application of asset definitions only to assets that are located within Australia (as per proposed subsection 9(2B)), further confuses the potential application to digital elements of critical infrastructure entities that have parts of their functional infrastructure or data located offshore, as mentioned above.

2.53 This variation in definitional breadth and specificity has caused many submitters and witnesses to express concern regarding the directed impact of the proposed framework from the SOCI Bill, or the unknown impact, which leads to a lack of industry confidence or an inability to accurately forecast regulatory impact and cost. Water Services Australia expressed:

> The water sector hasn't been consulted in detail about the costs. It's very hard to get a cost at the moment because we don't actually know the details of the rules—it's 'How long is a piece of string?' That's been problematic for us.[17]

2.54 The data storage and/or processing sector raised specific concerns with the definition of their sector, as well as the impact on their business given the 'horizontal' nature of their services, as they may provide data services to businesses captured under other asset sectors, and therefore be affected by the cyber focus of the Bill, not only for their own operations, but in relation to the services provide to those industries as well.

2.55 This point was made in opening statements at the public hearing of 8 July 2021[18] and expanded on by Mr David Masters, Director of Global Public Policy at Atlassian:

> …we are a horizontally enabling sector across all of these industry verticals. As you are thinking about the regulatory mechanisms, generally they will flow down to us as supporting services to those critical infrastructure sectors. I

---

17 Dr Greg Ryan, Director, Business Excellence, Water Services Association of Australia, *Committee Hansard,* Canberra, 8 July 2021, p. 51.

18 *Committee Hansard,* Canberra, 8 July 2021, pp. 1-10.

> think one of the concerns that we have as an industry is that the regulatory making process, the rule-making process that the Department of Home Affairs has flagged, needs to be considered as part of that process. Those regulatory requirements will flow down to us regardless of what they impose upon our sectors separately. I am just making sure that that is front of mind and also reflected in the bill, because some of the requirements that we see for other sectors—electricity or water or transport—may potentially be in conflict with what those sectors might be asking us to do separately as customers.[19]

2.56 A number of industry representatives identified that defining assets in the broad terms within the SOCI Bill did not provide for the realities of the operation of a number of the affected sectors. Instead, the suggestion for defining industry functions was a more practical step to protecting the data and functions that are essential to the operation of critical infrastructure assets:

> What we are asking basically is to zoom out and ask first: what do we want to protect and why? We sometimes ask our customers to engage in data classification. So when you identify highly sensitive data, what is top secret and what is just kind of general data that deserves protection but doesn't need the highest level of priority? I guess what we're arguing for is that governments need to start with workload classification. They need to identify the workloads that matter as opposed to specific assets. A practical example of this is to take a power company or even a government entity. There are several workloads that happen for that entity and one of them may be the cafeteria ordering system, for example, and another one may run the electric grid. Both of those workloads are not the same. If you prioritise both equally you're being over inclusive, you're diverting resources and you're also diverting regulatory resources on how to best protect that. What we are arguing for is, first, to step back, identify the functions that are really important to the Australian economy and the Australian industry and then figure out how to prioritise those functions, how to best protect those functions, so we can reduce regulatory costs for customers, for industry and for the government. This is a little bit of a different approach to identifying specific assets but we think this is a better approach.[20]

2.57 The definitions of sectors and assets is crucial to the operation of the SOCI Bill's proposed framework, and fundamentally establishes the areas of the

---

19 Mr David Masters, Director of Global Public Policy, Atlassian, *Committee Hansard,* Canberra, 8 July 2021, p. 11.

20 Mr Hasan Ali, Assistant General Counsel, Office of Critical Infrastructure, Microsoft, *Committee Hansard,* Canberra, 8 July 2021, p. 19.

Australian economy, and international partners operating within Australia in relevant sectors, that are affected, or will be affected by the Bill.

Unknown regulatory burden of positive security obligations

2.58 As outlined earlier, an overwhelming concern from industry representatives was the unknown nature of the majority of the regulatory impact or burden to be imposed by the proposed new Parts 2A-2C, and to some extent those in the proposed new Part 3A, of the Bill.

2.59 While the SOCI Bill outlines and defines the types of obligations and some of the elements of those obligations that industries will have to comply with, most of the detail of what businesses will have to do, and by what means is not prescribed in the Bill. Again, this detail is proposed to be designed and outlined in rules to be presented in delegated legislation.

2.60 Without certainty regarding definitions and regulatory requirements, affected industries cannot plan for the potential impact and cost of the framework's requirements, as highlighted by Google:

> From Google's perspective I'd like to say that many of the points we'd make have already been made here, but there's one—clarity—when it comes specifically to your question of costs. One of the ways to reduce cost is to ensure that there's clarity. Some of the concerns that we've raised, especially around reporting arrangements and definitions, can without clarity inadvertently cause great costs, as when we're responding to an incident or having to deal with an issue we have uncertainty about what is covered, when something is covered and what the time frame is. Making sure all the definitions in this bill are very clear and appropriate is one of the best ways to reduce costs and make sure that we get the best possible outcomes.[21]

2.61 While this process of designing rules outside of the legislation is identified as providing for flexibility and consultation, most industry submitters expressed a preference for this detail to be included in the primary legislation, or that detail to be negotiated and provided in instruments to be considered alongside an amending Bill before the framework be considered and passed through Parliament.

2.62 The National Pharmaceutical Services Association summed up many of the concerns from industry in its opening statement to the 9 July public hearing:

---

[21] Mr Shane Huntley, Director, Threat Analysis Group, Google Security, Google, *Committee Hansard*, Canberra, 8 July 2021, p. 11.

> Like others appearing today, NPSA members are rightly cautious about a Bill that provides nothing more than a skeleton framework of broad ranging and extensive powers and being told the rest will be worked out later by the Department of Home Affairs and the Minister through co-design.
>
> Trusting in these statements is a significant leap of faith given what we would respectfully argue is a lack of consultation to date and an impossibly tight 2-week window for consideration of 129 submissions on the draft Bill before its tabling by the Minister.
>
> The legislation is too thin on detail. It is impossible to know what its implications will be for NPSA members, and the proposed mechanisms within the Bill would make it almost impossible to challenge.
>
> We believe that this is too great a risk given the scope of the proposed powers, and we recommend that the details of the regulatory framework must be within the primary legislation, not in rules and determinations.[22]

Potential duplication of regulatory systems

2.63 In addition to the concerns regarding the unknown elements of regulatory impact, a number of industry representatives expressed concern regarding potential duplication of existing regulatory systems.

2.64 Some entities expressed very strong opposition to any further form of regulation that might duplicate or supplement existing obligations. Commercial Radio Australia highlighted this opposition, and potential consequences, in its opening statement to the 9 July public hearing:

> CRA seeks confirmation that the rules will provide, under section 30AB(3), that Part 2A will not apply to the commercial radio industry and the SOCI Act obligations will therefore remain dormant, with the industry's existing obligations continuing to apply without supplement.
>
> The commercial radio industry will resist strongly any attempt to impose additional compliance or reporting burdens on it through the Positive Security Obligations proposed in Part 2A (or any other part) of the Bill.
>
> If it is not possible to guarantee that no additional compliance or reporting obligations will be imposed on commercial radio, then the commercial radio industry would prefer that the Bill does not cover commercial radio infrastructure. Additional regulations would threaten the viability of

---

22 National Pharmaceutical Services Association, *Committee Hansard*, Canberra, 9 July 2021, p. 50.

> commercial radio stations, to the detriment of local Australian audiences. Ultimately, this could reduce the critical infrastructure available for the communication of emergency information to regional Australians.[23]

2.65 This concern is ameliorated by the undertakings and identification in the SOCI Bill and Explanatory Memorandum that when defining rules the Minister must take into account any existing regulatory systems that provide for similar mechanisms. This is to ensure that regulation is not duplicated and was affirmed and restated in the Department's supplementary submission[24] as well as by the Secretary during the public hearing of 29 July 2021.[25]

2.66 Despite the mechanisms built into the SOCI Bill and the undertakings for co-design and avoidance of duplication, industry representatives made a call for existing regulators to be central to any design process, with the Business Council of Australia[26] and others calling for the Treasurer, or other relevant portfolio Ministers relevant to sectors, to be involved in any rules design and approval processes.[27]

Timeframes for notifications

2.67 Another recurring theme of evidence from industry representatives related to the timeframes outlined in the SOCI Bill for the notification of cyber security incidents under proposed Part 2B.

2.68 Proposed sections 30BC and 30BD require that entities must notify the relevant authority of any critical or other cyber security incidents (a cyber security incident is defined in proposed section 12M), within 12 and 72 hours respectively.

2.69 This timeframe is identified as having been modified from an original proposed 24 hours for general notifications from the exposure draft of the Bill[28], to the 72 hour period requirement, to align with existing similar

---

23 Commercial Radio Australia, *Committee Hansard*, Canberra, 9 July 2021, pp. 47-48.

24 Department of Home Affairs, *Submission 59.1*, pp. 39-40.

25 Mr Michael Pezzullo AO, Secretary, Department of Home Affairs, *Committee Hansard*, Canberra, 29 July 2021, p. 7.

26 Business Council of Australia, *Submission 75*, p. 4.

27 *Committee Hansard*, Canberra, 8 July 2021, p. 63.

28 Department of Home Affairs, *Submission 59*, p. 19.

requirements in schemes such as that regulated by the Australian Prudential Regulation Authority (APRA).

2.70 A number of submitters and witnesses, especially those from within the technology sector, expressed concerns regarding the nexus between the requirements of assessing the criticality or seriousness of a cyber security incident, and the requirement to notify the appropriate authority of such an incident within 12 hours.

2.71 In response, the Department outlined that the intention for notification for critical incidents is intended to be the initial commencement of a process, not the only process involved. Mr Hamish Hansford, First Assistant Secretary, Cyber, Digital and Technology Policy stated:

> I think the very first point of the 12 hours is to start a conversation, and so in the 12-hour threshold you've got to fulfil the legislative requirements. Effectively, the clock doesn't start when something happens; it's when you become aware that you have an incident and it falls within the category. The more detailed information about the content of the notification will fall in the rules, which will be subject to co-design. But the first notification can be oral and then subsequently, within 48 hours, it must be given in written form.[29]

2.72 These notifications play a vital role in establishing or catalysing a number of actions and records under the SOCI Bill's proposed framework. However, with the current lack of certainty around the metrics for assessing impact for the purposes of reporting incidents (as the seriousness or criticality of an incident is currently assessed according to impact under the Bill), there is concern regarding whether an entity will be in breach of the requirements of the Bill (with associated penalties) when assessment of the impact of an incident is based on elements such as availability, integrity, reliability or confidentiality, without accompanying thresholds for assessing restriction on these elements.

2.73 The Explanatory Memorandum provides limited guidance for entities:

> Determining whether an incident is having a significant impact on the availability of the asset will be matter of judgment for the responsible entity. The services being provided by the asset, together with the nature and extent of the cyber security incident, will determine the significance of the incident and whether it meets the threshold of being a critical cyber security incident. For example, a cyber security incident which affects the availability of a critical

[29] Mr Hamish Hansford, First Assistant Secretary, Cyber, Digital and Technology Policy, Department of Home Affairs, *Committee Hansard*, Canberra, 11 June 2021, p. 35.

> clearing and settlement facility for a very brief period may have significant economic repercussions while an incident that affects the availability of a critical education asset for the same period of time may have a substantially lower impact.[30]

Authorisations and executive powers

2.74 The proposed framework set in the SOCI Bill imposes very serious obligations on entities, as well as the potential for quite intensive assistance powers that allow for access to proprietary systems and IT architecture.

2.75 While the rationale behind the proposed framework is acknowledged by most stakeholders, the potential reach of the powers is not accompanied by appropriate authorisation or oversight mechanisms in the eyes of some.

2.76 Currently the authorisations for all proposed mechanisms sit solely within the Executive, either directly with Ministers or the Secretary of the Department (or delegated staff in limited circumstances).

2.77 The Law Council of Australia commented extensively on the potential powers proposed within the SOCI Bill and the potential for non-disclosure of significant items of interest:

> …the Bill is extraordinary in terms of the number, breadth and gravity of legislative powers it proposes to delegate to the Minister and Secretary. The Law Council submits that the Bill is fairly characterised as a 'framework' or 'shell' which imposes highly significant regulatory obligations and liabilities, but largely delegates to the executive government the task of determining the substance of regulatory requirements, and their application to specific entities.
>
> The Bill is also extraordinary in that it proposes to enable some delegated powers to be exercised via non-legislative instrument (Ministerial declarations in relation to assets, and Secretary's notices in relation to cyber security obligations). These determinations and notices will not be disclosed publicly, with disclosures of their existence or contents potentially attracting the secrecy offence in section 45 of the SCI Act. They will also bypass the usual requirements for Parliamentary scrutiny and disallowance that apply to legislative instruments under the Legislation Act.[31]

2.78 The Law Council and others also commented on the current exclusion of any independent authorising officer or potential check against the notices or

---

30 Explanatory Memorandum, p. [122].

31 Law Council of Australia, *Submission 64*, p. 23.

obligations and directions that could be issued under the Bill's proposed frameworks.

2.79 While the proposed framework would fall under the jurisdiction of the IGIS, Commonwealth Ombudsman and OAIC, to varying degrees, the SOCI Bill proposes to exclude from statutory judicial review all administrative decisions made under the intervention regime in proposed Part 3A in relation to cyber security incidents.

2.80 This proposed exclusion is based on national security grounds, but excluding these potentially far-reaching elements of the Bill from any review has instigated a call for some form of review of decisions, whether by a panel of experts, such as that provided for under Part 15 of the *Telecommunications Act 1997*[32], or ex post facto judicial review of the grounds a Ministerial authorisation is based upon.[33]

Government assistance measures

2.81 Proposed Part 3A assistance powers are the portion of the SOCI Bill that has been expressed as being the most urgent, but are also those which generated significant concerns by industry during the inquiry.

2.82 The ability for the Minister to authorise the Secretary of the Department to direct an entity to gather information, undertake an action (or direct that an action not be undertaken), or authorise ASD to intervene, when a cyber security incident has occurred, is occurring, or is likely to occur, is a considerable power to wield under the proposed framework for security of critical infrastructure.

2.83 While the Minister must take into account a number of factors when considering authorising a government assistance direction, including seeking the agreement of the Prime Minister and the Defence Minister in relation to intervention requests, the range of actions available under proposed section 35AC for interventions, as well the considerable penalties that apply to non-compliance, and the potential for liability, are areas of concern for many stakeholders.

2.84 These government assistance measures are identified as provisions of 'last resort' throughout the Explanatory Memorandum, but many witnesses at

---

32 Telstra, *Submission 56*, p. 4.

33 .au Domain Administration, *Submission 74*, pp. 14-15.

the public hearings of 8 and 9 July 2021 questioned whether the measures allowed for would indeed be used only in the direst circumstances.

2.85 In response, the Secretary of Home Affairs stated:

> On 8 and 9 July, earlier this month, the committee heard witnesses from many companies speaking of their cyber maturity. We observed those proceedings very closely, and they evidenced their willingness to engage voluntarily with the Australian Cyber Security Centre in a crisis. In such circumstances there would be no requirement for these powers to be utilised, and the government's first preference, as stated in the explanatory memorandum and elsewhere, of working collaboratively and in partnership with the entity would of course suffice. However, the risks to Australia's national interests, in the view of the government, are too great to not have a clear, established framework in place ahead of an incident to operate as a last resort in a national emergency, should an entity be unwilling or unable to do what is necessary.[34]

2.86 The references by the Secretary regarding entities and companies being willing to cooperate voluntarily with the ACSC aligns with the evidence received for the review, where most submitters and witnesses outlined willingness to cooperate, and pre-existing healthy relationships with ASD and existing relevant regulators.

2.87 This was summed up by Ms Rosemary Sinclair, Chief Executive Officer of .au Domain Administration Limited:

> We have a very close relationship with the Department of Infrastructure, Transport, Regional Development and Communications. We already work very, very closely with the Signals Directorate and the Australian Cyber Security Centre.
>
> So all those relationships and processes are in place. One of the things that strikes us about the legislation is that it's focusing on a problem of the unwilling and trying to address that, whereas I suspect that the people on this call and the vast majority of people who have been engaging in this process are in fact the willing. So we need to be careful about a response to the wrong problem.[35]

---

34 Mr Michael Pezzullo AO, Secretary, Department of Home Affairs, *Committee Hansard*, Canberra, 29 July 2021, p. 2.

35 Ms Rosemary Sinclair, Chief Executive Officer, .au Domain Administration Limited, *Committee Hansard*, Canberra, 8 July 2021, p. 33.

Committee comment

2.88 The Committee acknowledges the substantial and varied evidence received from all manner of submitters and witnesses to this Bill review. With this substantial and varied evidence comes an equally substantial and varied level of agreement and disagreement about the response required.

2.89 Outlined above is a brief snapshot of the main themes of evidence received from the majority of submitters and witnesses. The Committee is unable to outline all the evidence received, and as will be discussed in the next Chapter, does not believe it is relevant to do so at this stage.

2.90 The uncertain regulatory cost is an element of the proposed framework that poses a substantial concern for affected industry. The fragility of the economy in an uncertain COVID-19 affected environment is a primary concern for the companies that will become critical infrastructure entities under the Bill, so any uncertainty in regulatory administration, cost or penalty is only going to heighten an already stressed commercial reality.

2.91 The Committee's proposed way forward is discussed in the next Chapter.

Challenges faced by the Committee with the reviews

2.92 The Committee has faced some challenges in being able to review the SOCI Bill in a timely and accurate manner.

Timing of referral

2.93 The first challenge came from the timing of the SOCI Bill's introduction to Parliament. With the SOCI Bill being introduced on Thursday, 10 December 2020, the final sitting day of that year, the Committee faced logistical pressure in launching the inquiry in the face of the Christmas period, where traditionally many stakeholders have reduced staff and ability to respond to a call for evidence.

2.94 To acknowledge this the Committee set Friday, 12 February 2021 as the due date for submissions, which even though there was a nine week period between the launch and requested due date, a number of submitters did not meet. Accompanying this was the fact that two other Bill inquiries had been launched by the Committee in December with the same due date and a lot of the non-government organisations that provide valuable submissions to the Committee for each of its inquiries, such as the Law Council of Australia, were overwhelmed with the call for evidence on multiple topics at once.

Confusion regarding consultation processes

2.95 As the Committee started to receive submissions it became evident that the consultation processes undertaken by the Department prior to the introduction of the SOCI Bill to Parliament had created some confusion for potential and actual submitters.

Cyber Security Strategy 2020 to Bill introduction

2.96 Between September 2019 and February 2020 the Department consulted on the development of Australia's Cyber Security Strategy 2020 (the Strategy). The final report was publicly released in late July 2020.

2.97 Resulting from the Strategy, the Department released the *Protecting Critical Infrastructure and Systems of National Significance Consultation Paper*, first proposing the framework which is now embodied in the SOCI Bill. Consultation processes on this paper:

> …revealed broad in-principle support for the introduction of the reforms. Certain sectors strongly supported their inclusion within the proposed coverage of the framework, given their level of criticality and currently limited regulatory environment. Industry concerns primarily centred on the sectoral implementation of the reforms including the need for greater clarity around coverage, true industry co-design of sector-specific requirements to reduce unnecessary regulatory impost, and the extent of proposed Government Assistance powers. Industry further called for consultation on an exposure draft of the proposed bill.[36]

2.98 Out of this process the Department released an exposure draft of the Bill and associated documents on 9 November 2020 for comment. This was followed by further industry consultation, closing on 27 November 2020.

2.99 The SOCI Bill was then introduced to the House of Representatives eight business days later on 10 December 2020. Further commentary on this timeframe is provided later in this report.[37]

---

[36] Department of Home Affairs, *Submission 59*, p. 18.

[37] More detail on the consultation processes undertaken by the Department can be found at https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-critical-infrastructure-systems, or at pages 17-19 of the Department's primary submission No. 59.

Effect on Committee submissions

2.100 The effect of the rapid process outlined above was that when the Committee started to receive submissions, a number of them did not expressly address the Bill before the Parliament or the statutory review. Many expressed the same feedback provided to the consultation process conducted by the Department, with many attaching copies of submissions made to both the consultation paper and Bill exposure draft processes, even though minor but technically consequential amendments had been made to the SOCI Bill since those submissions had been written.

2.101 Similarly, the Committee did not receive the expected quantity of submissions from affected companies from the critical infrastructure asset sectors or the peak-bodies that represent those industries. This was despite a request from the Committee to the Department in early January 2021 to avail their submitters of the Committee process underway, which the Committee was advised had occurred.

2.102 In later interactions with witnesses, through direct communications with witnesses, or through lobbying from companies once public hearings were announced in June and July 2021, it became evident that many organisations were either not aware of the Committee process, or had assumed that the input provided to the Department would constitute evidence to the Committee. A number of late submitters also expressed a feeling of 'consultation fatigue' or voiced concerns that earlier feedback had made little or no impact on the final SOCI Bill presented to Parliament.

Committee workload

2.103 The workload of the Committee in 2021 has also been a challenge in considering the SOCI Bill.

2.104 For the majority of 2021 the Committee has had a revolving inquiry load averaging between 10 to 15 active inquiries at any one time, with the Committee having handed down ten reports or statements finalising various inquires, reviews or terrorist organisation listings under the *Criminal Code* in that time, with 25 finalised in total for the 46th Parliament to date.

2.105 This workload and the requirement for associated public hearings, briefings and meetings places strain on the Committee to be able to undertake the appropriate evidence gathering and consideration of such evidence. As outlined earlier in this Chapter, the evidence base for this Bill review and the range of affected industry entities is extensive.

Evolving evidence base and contemporary regulation development

2.106 The restricted evidence base in the early stages of the Bill review did reduce the range of industry opinions that were presented to the Committee somewhat, but this evidence advanced and expanded as time progressed and affected companies and representative bodies became aware of the process.

2.107 However, the Committee received a range of submissions prior to, during hearings and after, mainly due to the engagement related to these processes, but also due to the evolving nature of feedback from submitters.

2.108 As discussed, the Department engaged in industry consultation during 2021, in parallel to the Committee's inquiry, in line with the co-design process outlined in the SOCI Bill, Explanatory Memorandum, and as expressed in the 'timetable for implementation and key tasks' outlined in the Regulatory Impact Statement included at Attachment B of the Explanatory Memorandum.[38]

2.109 This co-design process for the rules to apply to certain elements of the SOCI Bill's proposed framework either instigated engagement with the Committee process (for industries that may have not been aware of the process, or who had assumed that the Committee was privy to earlier engagement with the Department), or reinvigorated or altered evidence provided to the Committee regarding the concerns expressed around a lack of consultation or the lack of detail regarding the regulation to be provided for in the rules being drafted.

2.110 The impact of this new evidence or the shift in existing evidence challenged the Committee in being able to settle its understanding of the concerns being expressed from industry.

COVID-19 lockdowns

2.111 Additionally, as the Committee conducted the last of its public hearings in July and collected the resultant evidence, or received new evidence from submitters catalysed by those hearings, the further lockdowns in Sydney, Melbourne and Canberra seriously affected the Committee's ability to be able to collaborate on the evidence received and formulate a response.

2.112 This challenge and the increasing evidence from the Department and ASD that the threat of cyber security vulnerability of critical infrastructure assets

---

38 Explanatory Memorandum, pp. 293-294.

was escalating and needed urgent response has necessitated the form and substance of this report and the recommendations in Chapters 3 and 4.

3. Facing the immediate threat - Committee comment

3.1 As the Bill review progressed, it became evident that the divided evidence base and divergent opinion between government and affected industry regarding the impact, scope and detail of the SOCI Bill, were going to be a restrictive factor in building stakeholder consensus in support of the proposed reforms.

3.2 As outlined in Chapters 1 and 2 most, if not all, companies and industry bodies, trade unions, and critical infrastructure assets owners and operators expressed some form of reservation with the Bill, its consultative development, the unknown or unquantifiable regulatory impact, or the contemporary rules development that has occurred while the Committee conducted this review.

3.3 These concerns have been acknowledged by the Department in a general way while endorsing very few suggestions for potential change to the proposed framework of the Bill. The Department's rationale for advising against amendments has often been based on the urgency of the response required to the threat faced by critical infrastructure assets.

3.4 The Committee has heard compelling evidence regarding the threats to be countered, as well as the instances of ransomware and other cyber attack that have seriously impacted critical infrastructure both domestically and internationally.

3.5 The disagreement on the content of the SOCI Bill, the unknown nature of the rules to dictate the majority of asset regulation, and the increasing importance of countering the ever-evolving cyber threat to Australia's social and economic stability, defence and national security, has highlighted to the

Committee that all of the concerns expressed regarding the framework proposed in the Bill cannot be resolved in a manner that would be acceptable to all parties, and dictates that the proposed framework be amended.

3.6 The significant detail left to be resolved by sector rules in delegated legislation instead of in the primary legislation does not allow the Committee, the Parliament, or the effected entities sufficient confidence of the full impact of the legislation.

3.7 The Committee acknowledges that the rationale for relying on co-design for the rules is to enable appropriate impacts to be consulted on and for existing regulation to be catered for. However, the fact that this process has been underway in parallel to the Committee's review of the Bill and Act, but has not yet been concluded for any of the designated eleven industries means the Committee cannot make meaningful recommendations for these parts of the Bill, nor endorse them. To do so would be to effectively grant a blank cheque.

3.8 While the Committee strongly supports the aims of the SOCI Bill, it would need a significant amount of re-drafting to pass in its entirety and respond adequately to many of the concerns expressed to it during this review. This would delay significantly the time-critical elements of the Bill.

3.9 It is not the Committee's role to re-draft bills. However, the following commentary and recommendations in this Chapter are provided to assist in meeting the immediate threats we face now, as well as the comprehensive response which the Committee believes is necessary but accepts will take longer to finalise.

Splitting the Bill

> … once the bill achieves royal assent as an act of parliament it allows us to activate certain emergency procedures under the government assistance measures, and it is those measures that, frankly, I would prefer to have on the statute books tonight.[1]

3.10 The above quote from Secretary Pezzullo, and many of the requests to pause entirely the SOCI Bill's passage through Parliament, have informed the path

[1] Mr Michael Pezzullo AO, Secretary, Department of Home Affairs, *Committee Hansard*, Canberra, 29 July 2021, p. 10.

that the Committee is recommending regarding the review of the Bill, as well as the statutory reviews of both the Act and the TSSR Regime under Part 14 of the *Telecommunications Act 1997*. The recommended actions for the Bill are outlined below and the related consequences for the statutory reviews conclude the report.

3.11 These recommendations are either specific to the SOCI Bill, or are principles-based recommendations for actions to enable the elements of the Bill that remain contested to be reformed or refined.

Retain Part 3A and enabling provisions

3.12 In order for the increasing threat of cyber-enabled crime and security threats to critical infrastructure assets to be countered, the Committee is recommending that the government assistance measures within proposed Part 3A of the Bill be separated out and amended so as to be passed as soon as practicably (referred to from hereon as Bill One).

3.13 The Committee understands that the Government wishes to legislate to respond to the growing threat environment as soon as possible, and this separation will enable this to happen.

3.14 This will allow for the Department, and ASD as the technical authority, to work with entities to ensure that cyber security incidents can be responded to in the most expeditious fashion, to ensure that critical infrastructure assets (and associated functions) are secured.

3.15 Relevant sections of Part 1 of Schedule 1 of the SOCI Bill will need to be retained to enable all definitions and meanings to apply, to allow for the expanded critical infrastructure sectors to be assisted by the proposed Part 3A operation.

3.16 Proposed Part 2B will need to be retained within Bill One to allow for the notification of cyber security incidents, to allow for assistance measures under proposed Part 3A to be engaged when required. Similarly any amendments to the existing Parts 4 and 5 of the Act will need to be retained for such engagement of those provisions.

3.17 Schedule 2 of the SOCI Bill will need to be retained to allow for the liability of ASD staff to be limited related to actions undertaken under the proposed Part 3A provisions. However, these provisions require some further consideration, as outlined later in this Chapter.

3.18 These provisions should be amended to ensure that the stated intentions of cooperation and reactive consultation are enabled by the provisions of Bill One. Capturing elements such as:

- the meanings of cyber security incident and unauthorised access, modification or impairment in proposed sections 12M and 12N be reviewed to ensure that an insider threat is captured;
- under proposed section 30BBA rules designed for the purposes of proposed section 30BB be published *and* advised directly to any identified affected entities or companies, and that feedback in submissions received be considered *and* responded to formally before the rules are then presented to Parliament;
- 'offensive cyber action' be defined on an inclusive basis for the purposes of the exclusions outlined in proposed Part 3A, so entities can know what the Minister is not authorised to require;
- 'significant impact', for the purposes of proposed section 30BC be defined, or clarified as part of the existing proposed section 8G definition of 'relevant impact'; and
- the consultation that the Minister is required to take under proposed section 35AD be required in a specific form, and to a reasonable timeframe to allow for the entity to reply before the ministerial authorisation is made.

3.19 Any other relevant or required amendments to allow for these separated out elements not outlined above can also be made and outlined in Bill One's explanatory material.

3.20 The remaining elements of the current SOCI Bill can then be deferred as a separate Bill, as per recommendations later in this Chapter.

Recommendation 1

3.21 The Committee recommends that the Security Legislation Amendment (Critical Infrastructure) Bill 2020 be split in two, so that the urgent elements of the reforms contained within the government assistance measures in proposed Part 3A, with the definitions and meanings of expanded critical infrastructure sectors and assets, and other enabling provisions contained within proposed amendments to Part 1, Part 2B, Part 4, Part 5 and Schedule 2 of the current Bill, be retained, amended in line with the principles outlined in paragraph 3.18 of this report, and legislated in the shortest time possible (Bill One).

3.22 The Committee acknowledges that affected entities will still have reservations with the enablement of the assistance measures, especially within the technology sector. However, the Committee recognises that the potential threat faced to critical infrastructure assets is too great to stall introduction of these essential measures for any longer.

3.23 In making these recommendations the Committee is relying on the intention stated in the SOCI Bill, and as outlined in evidence from the Department, that these measures will only be used as a last resort.

3.24 The Committee expects that given the statements from witnesses regarding a willingness for cooperation with the Department and ASD, and given the safeguards outlined in proposed section 35AB requiring the Minister to consider multiple impacts and current responses, then these measures will need to be used rarely, if at all. And if they are used, it will only be on those entities that are unwilling or unable to respond appropriately.

3.25 More comment and a recommendation regarding proposed Schedule 2 of the SOCI Bill is outlined later in this Chapter.

Notification requirements and timeframes

3.26 As outlined above, the positive security obligation set out in proposed Part 2B of the SOCI Bill (Notification of cyber security incidents), is required as part of Bill One, as entities are sometimes the only party aware that a cyber security incident is underway that requires the engagement of a proposed Part 3A government assistance measure.

3.27 In response to identified concerns regarding the 12 hour timeframe that notifications would be required for critical incidents, the Committee believes that the 12 hour notification is reasonable, given the ability for such a notification to be made orally in the first instance, but believes that the current requirement for the entity to then issue a written report within another 48 hours is too onerous. This is potentially complicated if the entity is still in the midst of determining what the incident may be and its effect.

3.28 Accordingly, the Committee is recommending that proposed section 30BC be amended to allow for the entity and the relevant Commonwealth Body (either ASD or another relevant regulator, as established under proposed section 30BF) to agree on the timeframe for a written report to be given, with a maximum of 84 hours from the time that the initial oral notification is given (96 hours total from the time that the entity becomes aware of the incident).

3.29 The amended section should also allow for a notification to be finalised without the need for a written record to be given, if the entity and the relevant Commonwealth body agree that the incident does not meet the definition of a critical cyber security incident. For consistency, the requirements of proposed section 30BD should be amended to allow for the finalisation of a non-critical incident notification by this means as well.

Recommendation 2

3.30 The Committee recommends that proposed Part 2B of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 be retained in Bill One, and that Part be amended to:

- **extend the requirement under proposed section 30BC for formal written notification to be made by an affected entity within 84 hours if an initial oral notification is given when a critical cyber security incident is having a significant impact on the availability of the critical infrastructure asset the entity is responsible for; and**

- **that proposed sections 30BC and 30BD be amended to allow for an entity and the relevant Commonwealth body to agree that a written notification is not required for an incident, if upon investigation it is agreed that the incident does not meet the requirement of an incident or does not have the defined impact outcome.**

3.31 The Committee understands that the substance of the form of the written notifications and the entities to be affected by this proposed Part are to be established in rules, so the Committee recommends that these rules be designed and agreed to included as part of the explanatory material for Bill One, or as soon as possible after Bill One is passed. This way, entities will know whether they are specified in such rules and what form a notification must take, especially given that the penalty for non-compliance is set at 50 penalty units (currently $11,100).

Recommendation 3

3.32 The Committee recommends that the rules to be designed for the purposes of amended Part 2B of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 be developed in consultation with relevant entities and incorporated into explanatory material to Bill One.

3.33 In order for the Parliament, and through it the Australian public, to be satisfied that the government assistance measures are being used in line with the last resort expectations of usage, the Committee is also recommending that any determination made under the Part 3A powers enabled by Bill One be reported to the Committee as soon as practicable after the assistance is rendered.

3.34 This report should be provided initially in written form outlining the circumstances and entities involved, the assistance measure used and the current status of the incident and any outstanding actions or results.

3.35 The Committee can then receive extra information in briefings from the Department, ASD or any other relevant Commonwealth Body. This will also allow for the Committee to request meetings or briefings from the affected entity or entities as well, to ensure that the assistance was requested, notified and undertaken in an appropriate and lawful manner.

Recommendation 4

3.36 The Committee recommends that Bill One include a provision that as soon as practicably after a government assistance measure is directed or requested the Parliamentary Joint Committee on Intelligence and Security be notified in writing about the circumstances, actions, status and parties involved in each measure used relative to any cyber security incident.

3.37 The IGIS and Ombudsman will continue to have oversight and complaints investigation roles to the measures within Bill One, adding that extra level of assurance that the powers are being used appropriately, and any complaints or concerns are given adequate avenue for recourse.

3.38 Once the amendments have been made, the Committee recommends that Bill One be passed.

Recommendation 5

3.39 The Committee recommends that, subject to the amendments outlined above, the resultant Security Legislation Amendment (Critical Infrastructure) Bill (Bill One) be passed.

Expanded role for the Cyber and Infrastructure Security Centre

3.40 The Committee received correspondence from the Secretary dated 30 August 2021[2] outlining changes to the existing Critical Infrastructure Centre (CIC), creating the Cyber and Infrastructure Security Centre to:

> …lead the Australian Government's efforts to protect Australia's critical infrastructure through an all hazards security and resilience regulatory mandate. The Cyber and Infrastructure Security Centre will bring together the Department of Home Affairs regulatory capabilities on aviation and maritime security, critical infrastructure security, and the background checking function performed by AusCheck with an expanded and integrated mission.[3]

3.41 This reformed body within the Department is a welcome move and consolidates advice and regulatory functions under multiple Acts, and this potential reformation of the CIC was flagged by the Secretary in evidence:

> Of the three big tools we have, the critical infrastructure centre, which goes to infrastructure security, was born out of a physical infrastructure security legacy, but I'm thinking about how I reconfigure administratively a cybersecurity and infrastructure security function.[4]

3.42 As the Committee is cognisant of potential concerns about the impact of Bill One from potentially affected entities, the Committee is recommending that the role of the expanded Cyber and Infrastructure Security Centre be further expanded, to be used as a technical review mechanism for the purposes of Bill One.

3.43 This reformed role would serve as a third-party checking mechanism regarding the suitability and feasibility of assistance measures, with industry and ASD technical experts convened as a technical expert advisory function within the Centre, enabled for both the Minister or Department and affected entities to seek advice on the assistance measures or circumstances surrounding the cyber security incident that catalysed the measure.

---

2 Department of Home Affairs, *Submission 59.4*.

3 Department of Home Affairs, *Submission 59.4*, p. [1].

4 Mr Michael Pezzullo AO, Secretary, Department of Home Affairs, *Committee Hansard*, Canberra, 11 June 2021, p. 40.

Recommendation 6

3.44 The Committee recommends that the Cyber and Infrastructure Security Centre within the Department of Home Affairs, be reformed to additionally provide technical support and advice regarding the functions of Bill One.

Part 6A declarations and the remainder of the Bill

3.45 The Committee understands that the intention of the SOCI Bill is to address the risk of potential and real cyber vulnerability within critical infrastructure entities within Australia. However, for the reasons stated above, the remaining elements of the SOCI Bill, including the declarations of SoNS, need to be redeveloped through engagement with the asset sectors and entities potentially affected by the SOCI Bill's proposed framework as a whole. The responsibility for reinvigorating and amending these contested elements of the SOCI Bill should not fall on government alone.

3.46 The Committee understands that the intention of declarations of SoNS under proposed Part 6A enables the enhanced cyber security obligations under proposed Part 2C of the SOCI Bill; however the general consensus regarding both the positive and enhanced cyber security obligations and their unclear burden and impact, due to a reliance on yet to be designed rules, is not a tenable way forward at this time.

3.47 The Committee supports the intention of all of the measures outlined in the SOCI Bill, however it recognises that the evidence provided, and the reliance on designing rules after an enabling Bill was expected to be passed, highlights that the framework as a whole is not ready to be progressed at this time. This is especially important given the uncertain nature of economic, supply chain and infrastructure security during the current pandemic, and the regulatory certainty desired by entities, as highlighted by the Group of Eight:

> The red tape argument certainly is one that we believe in quite strongly. We really need to be very proportionate in how we regulate these types of issues so that we effectively use regulations to get the best outcome in terms of protecting critical infrastructure...we just need to be careful that we are regulating to best effect, if you like, and that we don't get overwhelmed with red tape, because there's an opportunity cost in a resource constrained environment from any kind of regulatory activity, and we want to make sure

that we're doing our best to get the best outcomes from these types of processes.[5]

3.48 Accordingly, the Committee is recommending that the remaining elements of the SOCI Bill not outlined above (or any elements not essential to the retention of the features mentioned) to be included in Bill One, be revisited and reconsidered by the Department, in consultation with potentially affected industry representatives, and reintroduced in a subsequent second Bill.

3.49 As part of this reconsideration and consultative redesign, the Committee recommends that additional Bill (referred to from hereon as Bill Two) be amended in line with the following principles, incorporating a number of thematic considerations and recommendations put forward by submitters such as the Business Council of Australia, Law Council of Australia, and other industry representative bodies or businesses:

- any definitions or meanings introduced by Bill One that have been clearly identified as requiring modification or clarification as part of rules co-design or in evidence to this review, or that require reconsideration as to scope, be captured in revised definitions;
- any elements of PSOs or enhanced cyber security obligations that can be aligned to international standards or to align with existing best-practice critical infrastructure programs in other international jurisdictions (ISO 31000 is an international risk management standard already applied by many entities)[6];
- any decision or determination made that will affect an entity be amended to not only include the existing consultation by the Minister or Secretary, but also require a right of reply by the affected entity and consideration of that reply in the final determination;
- consideration of potential impacts of Bills One and Two on foreign investment attractiveness and Foreign Investment Review Board processes;
- the currently drafted secrecy around declarations of assets as SoNS under proposed section 52B of the SOCI Bill, and current section 51 of the Act, be amended to require that such declarations only be

---

5 Dr Matthew Brown, Deputy Chief Executive, Group of Eight, *Committee Hansard*, Canberra, 9 July 2021, p. 39.

6 More information regarding the ISO standard can be found at https://www.iso.org/iso-31000-risk-management.html

confidential if the Minister is satisfied on reasonable grounds, that there is a significant risk of harm to Australia's defence or national security as a result of the disclosure of the regulatory status of the asset;

- ensure that protected information provisions enable the appropriate and lawful exchange of information among oversight and compliance assurance bodies;
- formulating a merits review system of appeal to the security division of the AAT for any determination under Bill Two for declarations under proposed Part 6A and proposed Part 2C, once revised, with requisite access to protected information;
- more generally, consideration of the issue of merits review rights in respect of the administrative decisions of the Secretary or Minister under other aspects of the expanded SOCI Bill framework; and
- reconsideration of the suitability of the types and breadth of immunities afforded to entities under the entirety of the SOCI Bill's proposed framework (including those in Bill One).

Recommendation 7

3.50 The Committee recommends that the remaining non-urgent elements of the current Security Legislation Amendment (Critical Infrastructure) Bill 2020 not recommended for inclusion in Bill One, be deferred and amended into a separate Bill (Bill Two) in line with the principles outlined in paragraph 3.49.

3.51 As outlined earlier, when amending Bill Two, the Committee recommends that the substance of the primary SOCI Bill be reviewed in consultation with key stakeholders (those that engaged with the Department's consultation process, those who engaged with this Committee review, and any other identified parties). Bill Two should then be released as an exposure draft for extensive consultation with affected industries and representative bodies, with follow-up consultation meetings to be held on the collective feedback received from that exposure draft process.

3.52 This process will allow for the collaborative intention of securing critical infrastructure assets, and bring a sense of ownership to the process from those entities that will ultimately have a regulated role under the final legislative framework.

3.53 When the draft Bill Two is then further refined based on that feedback, the substance of the feedback and resultant change to Bill Two should be clearly outlined in the explanatory memorandum. Once reintroduced to Parliament,

Bill Two should be referred to this Committee for review. Included with that Bill review, a review of the operation of the legislative changes from Bill One up to that date is to be conducted by the Committee at the same time, to ensure that it is operating as intended, and is indeed being used only as a last resort.

Recommendation 8

3.54 The Committee recommends that Bill Two be amended in consultation with key stakeholders, released for feedback and with further consultation on incorporated amendments based on that feedback, prior to being reintroduced to Parliament.

Once reintroduced, Bill Two should be referred to the Parliamentary Joint Committee on Intelligence and Security for review, with a concurrent review of the operation to date of the amendments to the *Security of Critical Infrastructure Act 2018* resulting from Bill One.

3.55 In addition to the amendment of Bill Two in line with the above, the Committee recommends that any rules to be developed be co-designed as part of the consultation process on Bill Two, to the extent possible, and be outlined in the explanatory memorandum to Bill Two once introduced.

3.56 This will allow for the fullest consultation and establishment of regulatory impact to be discussed and realised before the Parliament has to consider Bill Two enabling those rules. This will also allow for the realisation of the flexibility of having those elements of the critical infrastructure framework in instruments that can be amended, reviewed, or even disallowed, but also available for the Parliament and potentially affected entities to review alongside Bill Two.

Recommendation 9

3.57 The Committee recommends that any rules to be designed under Bill Two be co-designed, agreed and finalised to the extent possible before the introduction of that Bill and made available as part of the explanatory material for the Bill.

Criminal code amendments and IS Act amendments

3.58 The Committee understands the intention of the proposed amendments to the Criminal Code in Schedule 2 of the SOCI Bill. The uncertain nature of the work of ASD in intercepting and undertaking computer-related acts in the interests of national security is becoming more fraught as technology progresses.

3.59 These proposed amendments realise part of recommendation 74 of the *Comprehensive Review of the Legal Framework of the National Intelligence Community* (Richardson Review)[7], to enable ASD to undertake its mission and while in the proper performance of a function of that agency.

3.60 The Committee realises the intention of this Schedule and the immunities it would grant ASD, while also realising that the scope of that immunity will reach much further than the activities ASD would undertake as the technical authority for the purpose of the SOCI Bill and any amended Security of Critical Infrastructure framework.

3.61 The Committee acknowledges the detailed evidence that the Law Council of Australia tendered to the Committee on this issue[8], and while not necessarily agreeing that all of the Law Council's recommendations for amendment to this Schedule are warranted, the Committee does not believe that they should be not acted upon at all, as was suggested by the Department in its supplementary submission.[9]

3.62 Accordingly, the Committee is recommending that Schedule 2 of the SOCI Bill be reviewed with the concerns expressed by the Law Council of Australia in mind, and amended in Bill One taking into account the following principles:

- whether an immunity, rather than a defence of a mistake or ignorance of fact, is a more suitable mechanism to address potential accidental onshore acts. If so, articulate the preference in explanatory material;
- whether the proposed immunities are appropriate to extend to both criminal and civil liabilities, given the proposed expanded civil

---

7 Commonwealth of Australia, *Comprehensive Review of the Legal Framework of the National Intelligence Community - Volume 2 of 4: Authorisations, Immunities and Electronic Surveillance*, December 2019, p. 227.

8 Law Council of Australia, *Submission 64*, pp. 97-103.

9 Department of Home Affairs, *Submission 59.1*, pp. 28-30.

immunity leaves no recourse for affected entities to seek reparations for unintended damages;

- whether the expanded immunity could adversely impact on the warrant and issuing safeguards regarding interceptions and access to telecommunications and data under the *Telecommunications (Interception and Access) Act 1979* (TIA Act); and
- whether the expanded immunity should be expanded to include AGO and ASIS, as per the majority of recommendation 74 of the Richardson Review.

Recommendation 10

3.63 The Committee recommends that proposed Schedule 2 of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 be amended in accordance with the principles outlined in paragraph 3.62 and included as part of Bill One.

3.64 Some submissions to the review identified that as part of the consultation undertaken by the Department, draft regulations under section 13A of the *Intelligence Services Act 2001* (IS Act) were distributed for comment. These draft regulations have not been provided as part of the Bill review, but section 13A regulations are established to enable IS Act agencies to cooperate with and assist other agencies, subject to arrangements or directions given by the responsible Minister.

3.65 The proposed regulations identified the Department as a Commonwealth authority to be assisted by ASD under paragraph 7(1)(f) of the IS Act, but did not limit that assistance to the extent of proposed arrangements under the SOCI Bill. As identified by the Law Council of Australia and the IGIS, such regulations could potentially authorise ASD to assist the Department in relation to any of its functions under section 7 of the IS Act, such as collecting intelligence on people outside Australia.[10]

3.66 While the Committee is confident this would not be the intention of the regulations, and the Minister is capable of binding the agency to assistance as set out in arrangements or directions, the Committee agrees that there should not be any doubt as to whether the cooperation under section 13A is only for the purposes of actions expressly authorised by Parliament in

[10] Law Council of Australia, *Submission 64*, p. 63; Inspector-General of Intelligence and Security, *Submission 76*, pp. 3-4.

statute. The Department acknowledged this potential in its supplementary submission and identified that amendment to the IS Act would be required.[11]

3.67 Accordingly, the Committee is recommending that subsection 13A(2) of the IS Act be amended to restrict cooperation or assistance provided by an IS Act agency to agencies or other bodies under regulation outlined in subsection 13A(1) only to the functions and extent authorised by other Commonwealth legislation.

Recommendation 11

3.68 The Committee recommends that subsection 13A(2) of the *Intelligence Services Act 2001* be amended to restrict cooperation or assistance provided by an agency under that Act to agencies or other bodies by regulation outlined in subsection 13A(1) only to the functions and extent authorised by other Commonwealth legislation.

Democratic institutions as critical infrastructure

3.69 The Committee heard expert evidence during hearings about the 'corrosive' potential of any interference with electoral process and that, "longer-term, sustained assault on democratic institutions and the information environment … is harder to grapple with, with this kind of bill that is focused around tactical support to organisations when they're compromised".[12]

3.70 The Committee also heard from the former Director of the Cybersecurity and Infrastructure Security Agency in the United States, Mr Christopher Krebs:

> Our strategies have to be connected against countering disinformation as much as we do technically. This is important for critical infrastructure as well. If you go to the point about an uneven underinvestment for cybersecurity in the critical infrastructure community, there is virtually no investment in countering disinformation. Nowhere more important is that right now than in the deployment of COVID-19 vaccinations. We are seeing an active threat environment from Russia and China for vaccine diplomacy. We're also seeing

11 Department of Home Affairs, *Submission 59.1*, p. 18.

12 Mr Fergus Hanson, Director of International Cyber Policy Centre, Australian Strategic Policy Institute, *Committee Hansard*, Canberra, 9 July 2021, pp. 10–11.

it from conspiracy theorists and antivaxxers in general. There is a much longer tail on the disinformation.[13]

3.71 In the context of election security, Mr Krebs said that ahead of the 2020 Presidential election, the US Government prepared for technical attacks or disruptions to electoral systems and hacks against media websites and voter databases. But he warned that the 'more pervasive aspect' was the "…broader campaign… to undermine confidence in leadership, government and democratic institutions through disinformation operations".[14]

3.72 Mr Krebs confirmed to the Committee that government facilities are included as critical infrastructure in the United States, with election functions considered a specific subsection.

3.73 This evidence was put to department and agency representatives in subsequent hearings. The Secretary of the Department of Home Affairs, Mr Michael Pezzullo, advised that operational planning for the security of upcoming Australian elections was already underway and that, as the Australian Electoral Commission (AEC) was a part of government, specific legislation was not required to ensure the security of elections or to facilitate support from ASD or the Director-General of Security.[15]

Committee comment

3.74 Cyber-enabled operations spanning disinformation, data theft and technical disruption render democratic infrastructure vulnerable in new ways. Such operations, as witnessed in the 2020 presidential election in the United States, target political parties, news, and social media, and have the potential to affect broader public confidence in democratic systems.

3.75 The Committee notes the assurances from the Department of Home Affairs in relation to the AEC.

3.76 However, Committee members observe that democratic institutions in Australia are broader than the AEC and include State and Territory electoral commissions, a free press, local councils, State and Federal parliaments, and

---

13 Mr Christopher Krebs, Partner, Krebs Stamos Group, *Committee Hansard*, Canberra, 9 July 2021, p. 7.

14 Mr Christopher Krebs, Partner, Krebs Stamos Group, *Committee Hansard*, Canberra, 9 July 2021, p. 11.

15 Mr Michael Pezzullo AO, Secretary, Department of Home Affairs, *Committee Hansard*, Canberra, 29 July 2021, pp. 20 –22.

political parties. The Committee heard evidence that these institutions should be considered critical infrastructure.

3.77 The Committee appreciates that democratic institutions have characteristics which distinguish them in important ways from other entities; importantly, Australia has robust statutory mechanisms which protect the administration of elections from political interference from executive government. It can not automatically be assumed that a regulatory regime designed to secure critical infrastructure operated by business entities will be suitable to protect political parties.

3.78 Therefore the Committee is recommending that the Government review the risk of cyber threat to all levels of democratic institutions, to ensure that the most appropriate protections are in place.

Recommendation 12

3.79 The Committee recommends the Government review the risks to democratic institutions, particularly from foreign originated cyber-threats, with a view to developing the most appropriate mechanism to protect them at Federal, State and local levels.

Caretaker conventions, disinformation and cyber attacks

3.80 The Committee acknowledges the importance of Mr Krebs' observation that public officials, such as those from national security agencies, should be responsible for making any public notifications regarding cyber and disinformation threats, especially during election campaigns, in order to avoid perceptions of political influence:

> … you never want the incumbent with the ability to put their thumb on the scale and change the outcome of the election… you would not have wanted a White House press conference for those sorts of announcements because that, in and of itself, can be politicised.[16]

3.81 Evidence from the Department of Home Affairs confirmed that there is no requirement in Australia during the caretaker period for such information to be provided by a public official, or even for the incumbent government to

[16] Mr Christopher Krebs, Partner, Krebs Stamos Group, *Committee Hansard*, Canberra, 9 July 2021, p. 12.

advise or seek agreement from the opposition party prior to making such an announcement. Rather, any consultation during a caretaker period would be, "a matter for the Government".[17]

3.82 When questioned on this topic, the Department of Home Affairs Secretary advised the Committee:

> It would be always open to, the head of the government—that is, the Prime Minister—or a minister who has relevant competency, to make a decision about making an [public] announcement about any matter within their legal authority. Whether it related to a cyberattack, whether it related to a natural disaster, whether it related to any matter, that would always be open to a minister.[18]

Committee comment

3.83 Committee members observe that there are other conventions and rules in Australia's system of government that require government consultation with the opposition party on certain matters, particularly in relation to national security or in the context of an election.

3.84 Given that foreign interference, disinformation and cyber attacks are new risks to the free and fair conduct of elections in Australia, the Committee recommends that the caretaker conventions be updated to reflect this new context.

Recommendation 13

3.85 The Committee recommends the Government review the processes and protocols for classified briefings for the Opposition during caretaker periods in response to serious cyber-incidents, and consider the best practice principles for any public announcement about those incidents.

Concluding comments

3.86 As outlined above, the Committee believes that there is a critical need to legislate now the urgent measures proposed within the SOCI Bill. The Committee also recognises that there is not consensus about the impact of all

17 Department of Home Affairs, *Submission 59.1*, pp. 46, 49–50.

18 Mr Michael Pezzullo AO, Secretary, Department of Home Affairs, *Committee Hansard*, Canberra, 29 July 2021, p.21.

elements of the Bill. Rather than delay the time-sensitive elements of the Bill while other outstanding issues are resolved, the Committee has instead proposed this split to equip government now with the emergency powers it needs and give more time for the broader response to be settled with key stakeholders.

3.87 The recommendations made above are also the best result that the Committee feels can be reached given the significant constraints on this inquiry imposed by the Committee's workload, the limited time remaining in the Parliamentary sitting calendar and the COVID environment.

3.88 This response seeks to balance the immediate cyber threat to critical infrastructure assets with the ability for government assistance when the threat becomes real and unmanageable by critical infrastructure entities themselves, while also allowing for the next stage of the framework to be designed, agreed and implemented on a consultative and cooperative basis.

3.89 The Committee realises that this split amendment of the SOCI Bill may be somewhat difficult to follow, so the below table is provided for a visual representation.

Table 3.1 Recommended split-Bill response

Bill One – to proceed now (with recommended amendments)	Bill Two – to proceed later (after co-design and amendment)
Government Assistance Measures – Part 3A	Positive Security Obligations -Part 2A risk management programs
Notification requirements – Part 2B – with relevant rules	Enhanced Security Obligations – Part 2C
Critical asset definitions and meanings, or other enabling provisions	Declarations of Systems of National Significance – Part 6A
Schedule 2 – ASD Criminal Code Amendments	Any other amendments, including revised amendments from Bill One, as well as rules
IS Act amendment	

4. Statutory review and Telecommunications Sector Security Reforms

Statutory review of the *Security of Critical Infrastructure Act 2018*

4.1 As mentioned earlier in this report, the SOCI Bill and its referral coincided with the launch of a statutory review of the Act's operation to this date in its original form, as passed in 2018.

4.2 The requirements of the statutory review, as set out in section 60A of the Act, are to analyse the operation, effectiveness and implications of the Act and to:

- consider whether it would be appropriate to have a unified scheme that covers all infrastructure assets (including telecommunication assets) that are critical to:
  - (i) the social or economic stability of Australia or its people; or
  - (ii) the defence of Australia; or
  - (iii) national security; and
- review the circumstances in which any declarations have been made under Part 6 of this Act (declarations of assets by the Minister); and
- report the Committee's comments and recommendations to each House of the Parliament.

4.3 As mentioned in Chapter 1, even though the Committee requested submissions and evidence to the Bill review as well as the above statutory review, the overwhelming majority of evidence received was focused solely

on the SOCI Bill and did not identify any concerns with the current Act and its operation. The Department was effectively the only substantive submitter on the statutory review elements.[1]

4.4 The first area of focus for the statutory review, that was set by the Committee in its *Advisory Report on the Security of Critical Infrastructure Bill 2017*, is effectively made redundant by the expansions proposed in the SOCI Bill.

4.5 The second area for focus regarding declarations of assets as critical infrastructure assets was identified by the Department in its submission:

- 11 private declarations of critical infrastructure (at the date of the submission – February 2021);
- 168 assets on the register – 58 electricity, 20 ports, 61 gas, and 29 water.[2]

4.6 While the Committee was provided with these statistics, there was no detail provided as to the circumstances regarding why these declarations were made, except to the extent that the Minister considered the factors required by section 51 of the Act. The Committee did not pursue any evidence on these declarations, as the alteration of the Act proposed in the SOCI Bill became the primary focus of the conduct of the inquiry.

4.7 In a similar vein, the information gathering powers under section 37 of the Act and the directions powers under section 32 of the Act had not been used up to the end of 2020[3], so these elements of the Act were not pursued for inquiry by the Committee either.

4.8 Effectively, the only evidence received regarding the statutory review's scope were the statistics above, and the numbers of notifications received from reporting entities of assets included on the Register of Critical Infrastructure Assets – 748 to the date of the Department's submission.[4]

Committee comment

4.9 The Committee is mindful of its statutory duty to review the operation, effectiveness and implications of the Act, as required under section 60A of the Act. However, the introduction of the SOCI Bill and its effective

---

1 Department of Home Affairs, *Submission 59*, pp. 7-11.

2 Department of Home Affairs, *Submission 59*, pp. 9-10.

3 Department of Home Affairs, *Submission 59*, pp. 8-9.

4 Department of Home Affairs, *Submission 59*, p. 7.

alteration of elements of the Act that would be reviewed transformed the Committee's ability to undertake the review.

4.10 As outlined above and earlier in this report, the focus of submitters and witnesses was primarily on the Bill, and this required a parallel focus from the Committee as well. Trying to review the operation of an Act that had not had a number of its key provisions utilised, with a Bill to fundamentally amend that Act before the Committee as well, was a challenging exercise. Ultimately it was an exercise that the Committee could not undertake effectively in the face of overwhelming concern regarding the SOCI Bill's potential impact.

4.11 Accordingly, the Committee is using this report as commentary on the SOCI Bill with recommendations for change, as well as a vehicle for finalising the statutory review. However, the conclusions of the statutory review are that the shifting landscape that the Bill created did not allow for the statutory review to be analysed in a way that created an evidence base to meaningfully recommend any change. This is also reflective of the fact that the recommended changes from Bills One and Two will alter this landscape even further.

4.12 As a result, the Committee is finalising the current statutory review requirements under section 60A of the Act without any recommendations. However, the Committee is cognisant of the fact that the legislative changes from Bills One and Two will require further scrutiny once implemented. This is equally important given the indications by the Secretary that further critical infrastructure legislative change is envisaged for the future.[5]

4.13 Therefore the Committee is recommending that Bill One include the mechanism for a further statutory review into the operation, effectiveness and implications of the reformed security of critical infrastructure legislative framework. This review may be launched not less than three years after Bill One receives Royal Assent, to allow the Committee to tailor commencement to any timeframes regarding the Bills from this report and any further amendments to the legislation that the Government may introduce in the meantime.

4.14 The Committee envisages that any other amending legislation to the Act will be referred to it, therefore potentially requiring a maximum review launch period, as it may well be undertaking relevant Bill reviews in that period.

---

[5] Mr Michael Pezzullo AO, Secretary, Department of Home Affairs, *Committee Hansard*, Canberra, 11 June 2021, pp. 42-43.

4.15 Additionally, this further statutory review will enable the Committee to inquire into the ongoing nature of industry collaboration that is crucial to the success of the Security of Critical Infrastructure framework.

Recommendation 14

4.16 The Committee recommends that the Bill One include a provision that the Parliamentary Joint Committee on Intelligence and Security may conduct a review of the operation, effectiveness and implications of the reformed security of critical infrastructure legislative framework contained within the *Security of Critical Infrastructure Act 2018* not less than three years from when that Bill receives Royal Assent.

Review of Part 14 of the *Telecommunications Act 1997* – Telecommunications Sector Security Reforms

4.17 Much like the commentary above for the impact that the SOCI Bill had on the statutory review of the Act, the concurrent review that the Committee is undertaking into the TSSR regime has been unduly affected by the introduction of the Bill.

4.18 Section 315K of the Telco Act was introduced as a result of Recommendation 12 of the Committee's *Advisory report on the Telecommunications and Other Legislation Amendment Bill 2016*, requiring a statutory review to be commenced within three years of Royal Assent of that Bill.

4.19 Like the critical infrastructure statutory review, the operation, effectiveness and implications of the reforms were to be reviewed, along with:

- the security of critical and sensitive data,
- the adequacy of information-sharing arrangements between government and industry, and
- the adequacy and effectiveness of the administrative guidelines in providing clarity to industry on how it can demonstrate compliance with the requirements set out in the Bill.

4.20 These requirements reflected a summary of concerns regarding the Bill's potential effect at the time of that report, but much like the impacts outlined earlier in this Chapter, the introduction of the SOCI Bill affected the approach and focus of evidence tendered to the TSSR review, highlighting the potential impact of the SOCI Bill on telecommunications assets, as they are to be included as part of the communications sector covered by the Bill.

4.21 While this impact did not prevent submitters and witnesses from providing evidence to the TSSR review, it did alter the focus of evidence, with submissions and witnesses highlighting potential duplication of regulation or the unknown future state of the TSSR. The Department itself acknowledged that reforms to the Act were being developed in its submission to the TSSR review in November 2020.[6]

4.22 The Explanatory Memorandum to the Bill does acknowledge TSSR impacts:

> For the positive security obligations to apply to a 'critical telecommunication asset' a rule must be made by the Minister to turn the obligations on. The telecommunications sector already has robust security frameworks in place in the Telecommunications Act 1997, including obligations under TSSR in Part 14 of that Act. Reforms to the TSSR regime will be considered in 2021, to be informed by the Parliamentary Joint Committee on Intelligence and Security's 'Review of Part 14 of the Telecommunications Act 1997', and through consultation with industry.
>
> Government will consider the outcome of this Review before considering applying the SOCI Act's positive security obligations to the telecommunications sector. This will allow sufficient time to amend the Telecommunications Act 1997, if needed, and will avoid duplication of regulatory requirements on industry. However, retaining the definition of 'critical telecommunications' at this stage will clarify, for example, the telecommunications assets on which there must be a relevant impact to trigger the powers in Part 3A—Responding to serious cyber security incidents.[7]

4.23 Further evidence was tendered by the Department regarding interactions between the SOCI Bill and the TSSR regime in its submissions.[8]

4.24 Throughout all of the Department's evidence regarding the interactions between the SOCI Bill and the TSSR regime, the focus was on the Part 3A government assistance measures being made available to telecommunications assets under the Bill, but that other obligations would not be 'switched on' unless the TSSR regime was considered inadequate. This assessment would be further informed by, and based on, the outcomes of the Committee's review of the TSSR regime.

---

6 Department of Home Affairs, *Department of Home Affairs submission to the statutory review of Part 14 of the Telecommunications Act 1997*, November 2020, pp. 5-6.

7 Explanatory Memorandum, p. [32].

8 Department of Home Affairs, *Submission 59*, p. 10 and *Submission 59.1*, pp. 38-40.

Committee comment

4.25 The Committee is mindful of the statutory duties it is to fulfil with the statutory review of the TSSR regime. However, the same impacts on the critical infrastructure statutory review were evident to the process for the TSSR review. The crossover between the two is less than completely clear and the potential for regulatory duplication, and the industry's resultant hesitance, is evident.

4.26 Despite the indications regarding careful consideration, the Committee is unclear about the intention of the Department's management of the TSSR regime going forward given the following observation from the Secretary regarding potential regulatory duplication and whether an on-switch could be utilised:

> The safeguards are set out in the legislation. The decision-makers have to be satisfied—they can't do it on a whim—that the tests have been met, the thresholds have been met, and they include a lack of regulatory duplication. I will give you one counterfactual straight up, because the Department of Home Affairs is the regulator under the Telecommunications Act of the TSSR scheme. In fact it is on my pen, because the act sets out the responsibilities of both the minister and the secretary. I happen to be that officer, and I can tell you, Chair, and the rest of the committee, the TSSR is inadequate for this purpose. I can absolutely assure you, because we are the regulator.[9]

4.27 The Committee has concluded its review of the evidence provided for the TSSR review within the twelve month requirement set in section 315K of the Telco Act, and will report in the future with recommendations for potential reform to be considered and potentially implemented to improve the TSSR regime, and how that might interact with the *Security of Critical Infrastructure Act 2018* in the form it takes in the future.

Senator James Paterson

Chair

24 September 2021

[9] Mr Michael Pezzullo AO, Secretary, Department of Home Affairs, *Committee Hansard*, Canberra, 29 July 2021, p. 7.

A. List of submissions

1 Australian Risk Policy Institute

2 Mr Paul Wilkins

- 2.1 Supplementary to submission 2
- 2.2 Supplementary to submission 2
- 2.3 Supplementary to submission 2

3 Cybersecurity Coalition

- 3.1 Supplementary to submission 3

4 Griffith University

5 CAUDIT

6 Dr Brett van Niekerk

7 Active Cyber Defence Alliance

- 7.1 Supplementary to submission 7
- 7.2 Supplementary to submission 7

8 AGL

- 8.1 Supplementary to submission 8

9 Australian Signals Directorate

10 Australian Investment Council

- 10.1 Supplementary to submission 10

11 Optus

- 11.1 Supplementary to submission 11
- 11.2 Supplementary to submission 11

12 Atlassian

- 12.1 Supplementary to submission 12
- 12.2 Supplementary to submission 12

13 The University of Sydney

14 Microsoft

- 14.1 Supplementary to submission 14
- 14.2 Supplementary to submission 14

15 Australian Information Industry Association

- 15.1 Supplementary to submission 15

16 Information Technology Industry Council

- 16.1 Supplementary to submission 16

17 Australian Business Software Industry Association (ABSIA)

18 Maritime Union of Australia

- 18.1 Supplementary to submission 18

19 Asia Pacific Loan Market Association C/- Allens

20 Financial Services Council

21 Universities Australia

- 21.1 Supplementary to submission 21
- 21.2 Supplementary to submission 21

22 Mr Thomas Uren

23 Innovative Research Universities

- 23.1 Supplementary to submission 23

24 Coalition to Reduce Cyber Risk, Inc.

- 24.1 Supplementary to submission 24

25 BSA | The Software Alliance

- 25.1 Supplementary to submission 25

26 Sycon Security Consultants

27 AUCloud

- 27.1 Supplementary to submission 27
- 27.2 Supplementary to submission 27

28 The Electrical Trades Union of Australia

- 28.1 Supplementary to submission 28
- 28.2 Supplementary to submission 28

29 Property Exchange Australia Ltd

30 Cyber Security CRC

- 30.1 Supplementary to submission 30

31 Clean Energy Council

- 31.1 Supplementary to submission 31

32 BAI Communications Australia

33 AustCyber

34 Police Federation of Australia

35 Palo Alto Networks

- 35.1 Supplementary to submission 35
- Attachment 1

36 Australian Gas Infrastructure Group

- 36.1 Supplementary to submission 36
- 36.2 Supplementary to submission 36

37 Swinburne University of Technology

38 Office of the Victorian Information Commissioner

39 Commercial Radio Australia

- 39.1 Supplementary to submission 39

40 Risk and Insurance Management Society Australasia Limited

- 40.1 Supplementary to submission 40

41 Australian Industry Group

- 41.1 Supplementary to submission 41

42 WA Department of the Premier and Cabinet

43 Standards Australia

- 43.1 Supplementary to submission 43
- Attachment 1

44 Science & Technology Australia

45 Sunwater

46 Australian Banking Association

- 46.1 Supplementary to submission 46

47 The Group of Eight

- 47.1 Supplementary to submission 47

48 Australian Food and Grocery Council

49 Amazon Web Services

- 49.1 Supplementary to submission 49
- 49.2 Supplementary to submission 49

50 Water Services Association of Australia

- 50.1 Supplementary to submission 50
- 50.2 Supplementary to submission 50

51 Port of Melbourne Operations Pty Ltd

52 Maritime Industry Australia Ltd

- 52.1 Supplementary to submission 52

53 University of Melbourne

54 IoTAA

55 Ramsay Health Care Australia

56 Telstra

- 56.1 Supplementary to submission 56
- 56.2 Supplementary to submission 56
- Attachment 1

57 Pricewaterhouse Coopers

58 National Farmers' Federation

59 Department of Home Affairs

- 59.1 Supplementary to submission 59
- 59.2 Supplementary to submission 59
- 59.3 Supplementary to submission 59
- 59.4 Supplementary to submission 59

60 Asia Cloud Computing Association

61 Australian Technology Network of Universities and The University of Newcastle

- 61.1 Supplementary to submission 61
- 61.2 Supplementary to submission 61

62 Free TV Australia

63 Ports Australia

64 Law Council of Australia

- 64.1 Supplementary to submission 64

65 U.S. Chamber of Commerce

66 Australian Services Union

67 Qantas

- 67.1 Supplementary to submission 67
- 67.2 Supplementary to submission 67
- Attachment 1

68 Australian Institute of Superannuation Trustees

- 68.1 Supplementary to submission 68

69 Australian Custodial Services Association

70 Australian Council of Trade Unions

- 70.1 Supplementary to submission 70

71 Communications Alliance Ltd

- 71.1 Supplementary to submission 71

72 Office of the Australian Information Commissioner

- 72.1 Supplementary to submission 72

73 Google Cloud

- 73.1 Supplementary to submission 73
- 73.2 Supplementary to submission 73

74 auDA

- 74.1 Supplementary to submission 74

75 Business Council of Australia

- 75.1 Supplementary to submission 75
- 75.2 Supplementary to submission 75

- 75.3 Supplementary to submission 75

76 Office of the Inspector-General of Intelligence and Security

- 76.1 Supplementary to submission 76

77 Commonwealth Ombudsman

- 77.1 Supplementary to submission 77

78 *Confidential*

79 *Confidential*

80 FiberSense

- 80.1 Supplementary to submission 80

81 AVM John Blackburn AO (retd), Institute for Integrated Economic Research - Australia Ltd

82 Australian Logistics Council

83 National Pharmaceutical Services Association

84 Medicines Australia

85 Mr Tom Uren, Australian Strategic Policy Institute

86 Toll

87 Australian Institute of Company Directors

88 *Confidential*

B. List of witnesses at public hearings

Friday, 11 June 2021

Committee Room 2R1

Canberra

Law Council of Australia

- Ms Shannon Finch, Member, Corporations Committee, Business Law Section
- Ms Olga Ganopolsky, Chair, Privacy Law Committee, Business Law Section
- Dr David Neal SC, Co-Chair, National Criminal Law Committee
- Dr Natasha Molt, Director of Policy, Policy Division

Office of the Inspector-General of Intelligence and Security

- The Hon Dr Christopher Jessup QC, Inspector-General of Intelligence and Security
- Ms Bronwyn Notzon-Glenn, Acting Deputy Inspector-General
- Mr Steve McFarlane, Assistant Inspector-General
- Mr Brad Fallen, Acting Assistant Inspector-General

Commonwealth Ombudsman

- Ms Penny McKay, Deputy Ombudsman
- Mr David Fintan, Senior Assistant Ombudsman, Strategy Branch

Office of the Victorian Information Commissioner

- Mr Sven Bluemmel, Information Commissioner

- Ms Rachel Dixon, Privacy and Data Protection Deputy Commissioner

Office of the Australian Information Commissioner

- Ms Elizabeth Hampton, Deputy Commissioner

Department of Home Affairs

- Mr Michael Pezzullo AO, Secretary
- Mr Marc Ablong PSM, Deputy Secretary, National Resilience and Cyber Security
- Mr Samuel Grunhard, First Assistant Secretary, Critical Infrastructure Security
- Mr Hamish Hansford, First Assistant Secretary, Cyber, Digital and Technology Policy

Australian Signals Directorate

- Ms Rachel Noble PSM, Director-General
- Ms Abigail Bradshaw CSC, Head of the Australian Cyber Security Centre
- Mr Stephen McGlynn, A/g Deputy Director-General, Corporate and Capability
- Mr Karl Hanmore, First Assistant Director-General, Cyber Security Services
- Mr Dale Furse, First Assistant Director-General Partnerships, Engagement and Programs

Thursday, 8 July 2021

Committee Room 2R1

Canberra

Microsoft

- Mr Hasan Ali, Assistant General Counsel, Office of Critical Infrastructure

Atlassian

- Mr David Masters, Director of Global Public Policy

AUCloud

- Mr Phil Dawson, Managing Director

Google

- Mr Shane Huntley, Director, Threat Analysis Group, Google Security

Amazon Web Services

- Mr Philip Rodrigues, Head of Security, APJ Commercial
- Mr Roger Somerville, Director, ANZ Public Policy

Australian Information Industry Association

- Mr Ron Gauci, Chief Executive Officer

Information Technology Industry Council

- Courtney Lang, Senior Director of Policy

auDA

- Ms Rosemary Sinclair, Chief Executive Officer

Palo Alto Networks

- Mr Ryan Gillis, Vice President, Cybersecurity Strategy and Global Policy

Cybersecurity Coalition

- Mr Ari Schwartz, Coordinator

Active Cyber Defence Alliance

- Mr Andrew Cox, Steering Group Member
- Ms Helaine Leggat, Managing Partner, ICTLC Australia Pty Ltd

BSA | The Software Alliance

- Dr Jared Ragland, Senior Director, Policy APAC

Qantas Airways Limited

- Mr Luke Bramah, Qantas Group Chief Security Officer

Toll

- Mr Peter Stokes, President, Global Logistics
- Mr Berin Lautenbach, Global Head of Information Security

AGL

- Ms Elizabeth Molyneux, General Manager, Policy and Energy Markets Regulation

- Mr Louis Wellard, Senior Manager, Risk Assurance and Improvement Group Risk, Compliance and Insurance

Ports Australia

- The Hon Michael Gallacher, Chief Executive Officer

Water Services Association of Australia

- Mr Luke Sawtell, Manager Security & Resilience (Urban Utilities)
- Mr Greg Ryan, Director Business Excellence

Maritime Industry Australia

- Ms Teresa Lloyd, Chief Executive Officer

Clean Energy Council

- Ms Lucinda Tonge, Policy Officer

Australian Gas Infrastructure Group

- Mr Benjamin Wilson, Chief Executive Officer

Australian Banking Association

- Ms Rhonda Luo, Policy Director

Business Council of Australia

- Ms Jennifer Westacott AO, Chief Executive
- Mr Chris Louie, Senior Policy Adviser

Australian Investment Council

- Mr Brendon Harper, Head of Policy and Research

Australian Institute of Superannuation Trustees

- Mr David Haynes, Senior Policy Manager

Standards Australia

- Mr Jesse Riddell, Senior International Partnerships Manager
- Mr Adam Stingemore, General Manager, Engagement and Communications

Risk and Insurance Management Society Australasia

- Mr Brian Roylett, Director and Company Secretary

Australian Industry Group

- Mr Charles Hoang, Lead Adviser - Industry Development and Defence Industry Policy

Friday, 9 July 2021

Committee Room 2R1

Canberra

Australian Strategic Policy Institute (Via Video Conference)

- Mr Fergus Hanson, Director of International Cyber Policy Centre
- Mr Tom Uren, Fellow, International Cyber Policy Centre

Cyber Security CRC

- Ms Rachael Falk, Chief Executive Officer
- Ms Anne-Louise Brown, Director of Corporate Affairs

Coalition to Reduce Cyber Risk (Via Video Conference)

- Mr Alexander Botting, Director of International Policy

Institute for Integrated Economic Research - Australia (Via Video Conference)

- AVM John Blackburn AO (Retd), Board Chair

Mr Christopher Krebs (Via Video Conference), Private capacity

Maritime Union of Australia

- Mr Paddy Crumlin, National Secretary

The Electrical Trades Union of Australia

- Mr Michael Wright, Acting National Secretary
- Mr Cameron Humphreys, Delegate

Australian Services Union

- Mr Troy Dunne, Organiser (United Services Branch)

Australian Council of Trade Unions

- Mr Joseph Mitchell, Workers' Capital Lead

The Group of Eight

- Dr Matthew Brown, Deputy Chief Executive

Universities Australia

- Ms Catriona Jackson, Chief Executive

Australian Technology Network of Universities

- Mr Luke Sheehy, Executive Director

Innovative Research Universities

- Mr Conor King, Executive Director

Commercial Radio Australia

- Ms Sarah Kruger, Head of Legal & Regulatory
- Ms Joan Warner, Chief Executive Officer

Ramsay Health Care Australia

- Ms Katrina Cunningham, General Counsel and Company Secretary
- Mr Christopher Neal, Chief Information Security Officer

Telstra

- Mr James Toole, Government Relations Principal

Optus

- Mr Gary Smith, Head of Regulatory Compliance

Communications Alliance

- Ms Christiane Gillespie-Jones, Director Program Management (Via Teleconference)

Free TV Australia

- Mr Ross Mitchell, Director, Broadcasting Policy

National Pharmaceutical Services Association

- Mr Richard Vincent, Chair

Medicines Australia

- Ms Elizabeth de Somer, Chief Executive Officer

Australian Food and Grocery Council

- Dr Geoffrey Annison, Deputy Chief Executive

Thursday, 29 July 2021

Committee Room 2R1

Canberra

Department of Home Affairs

- Mr Michael Pezzullo AO, Secretary
- Mr Marc Ablong PSM, Deputy Secretary, National Resilience and Cyber Security
- Mr Samuel Grunhard, First Assistant Secretary, Critical Infrastructure Security
- Mr Hamish Hansford, First Assistant Secretary, Cyber, Digital and Technology Policy

Australian Signals Directorate

- Ms Rachel Noble PSM, Director-General
- Ms Abigail Bradshaw CSC, Head, Australian Cyber Security Centre
- Mr Stephen McGlynn, A/g Deputy Director-General, Corporate Capability
- Mr Karl Hanmore, First Assistant Director-General, Cyber Security Services

Additional comments by Labor members

Labor members agree with the Committee's report and endorse each of its recommendations.

We note that Part 3A of the bill will, if the Committee's recommendations are fully implemented, form the core part of "Bill One" – and, as recommended by the Committee, Bill One should be passed by the Parliament.

While Labor members support this approach, we share the concerns expressed by the Law Council of Australia and other submitters about the absence of independent authorisation, and the wholesale exclusion of statutory judicial review, in relation to the measures in Part 3A.

The Committee has not made any recommendations to address those concerns directly.

Under Part 3A of the bill, the Minister may (among other things) authorise the Secretary to give "information gathering" or "action" directions to the owners or operators of a critical infrastructure asset in response to a cyber security incident. The Minister may also authorise the Secretary to give an "intervention request" to the Australian Signals Directorate.

Under the bill, there is no independent issuing process for ministerial authorisations to exercise powers of intervention in cyber security incidents – and all decisions made under Part 3A would be excluded from judicial review under the Administrative Decisions (Judicial Review) Act 1977.

Labor members see merit in recommendations by the Law Council and other submitters that "[c]onsideration should be given to an independent issuing authority for authorisations to exercise powers of direction and intervention under

new Part 3A of the SCI Act, along the lines recommended by the third INSLM in relation to the authorisation of compulsory industry assistance powers under Part 15 of the Telecommunications Act" (Recommendation 12 of the Law Council's submission).

Moreover, in our view, in evidence tendered to the Committee the Government has yet to justify the wholesale exclusion of decisions made under Part 3A from judicial review under the Administrative Decisions (Judicial Review) Act 1977. In particular, the Government has not explained why the nuanced position put forward by the Law Council in Recommendation 26 of its submission should not be adopted.

If the Government implements the Committee's unanimous and bipartisan recommendations, the Committee will have a further opportunity to consider these and other matters during its review of "Bill Two". In our view, the Committee should take advantage of that opportunity and – in the absence of compelling evidence from the Government – recommend further improvements to Part 3A.

Hon Anthony Byrne MP
Deputy Chair

Hon Mark Dreyfus QC MP

Senator Jenny McAllister

Senator the Hon Kristina Keneally

Dr Anne Aly MP