Australian Government
Department of Home Affairs

Amendments to the *Security of Critical Infrastructure Act 2018* (Cth): Impact Analysis

Note on this Impact Analysis:

This document examines the case for reforms to the *Security of Critical Infrastructure Act 2018* (Cth), including the related costs and benefits of three viable options. It assesses the estimated regulatory impact of all options, with a particular focus on the regulatory option (being Option 2).

Industry consultation using a draft of this document has been conducted by the Department of Home Affairs to seek feedback on the impact of these reforms. This process aimed to provide transparency on the government's decision-making process and enabled regulatory impacts of options under consideration to be tested with stakeholders.

This consultation did not seek submissions on the suitability of the policy options considered or alternative approaches. These matters have been separately considered by the Department, which consulted with key stakeholders to support the resolution of these issues.

Consistent with Australian Government and Office of Impact Analysis guidelines, this Impact Analysis has been completed prior to the introduction of a Bill.

I. Executive summary 3

II. Introduction 6

1. What is the policy problem you are trying to solve and what data is available? 9

1.1 Growing number of cyber incidents which impact non-operational data storage systems held by critical infrastructure entities. 14

1.2 Businesses face difficulties responding effectively in the aftermath of an incident 16

1.3 No ability for the regulator to issue a direction to an entity to remedy a deficient RMP 18

2. What are the objectives, why is government intervention needed to achieve them, and how will success be measured? 21

2.1 What are the objectives? 21

2.2 Why should Government intervene? 21

2.3 How will success be measured? 23

3. What policy options are you considering? 25

3.1 Option 1: Maintain the status quo 25

3.2 Option 2: Amend the SOCI Act 26

3.3 Option 3: Enhanced collaboration with industry 30

4. What is the likely net benefit of each option? 32

4.1 Approach to determining costs and benefits 32

4.2 Likely net benefit assessment: Option 1 – Maintain status quo 33

4.3 Likely net benefit: Option 2 – Legislative Reforms 34

4.3.2 Benefits of Option 2 – Legislative Reform 45

4.4 Likely net benefit assessment: Option 3 – Enhanced collaboration with industry 47

5. Who did you consult and how did you incorporate their feedback? 49

5.1 Purpose and objectives of consultation 49

5.2 Summary of consultation completed 49

6. What is the best option from those you have considered and how will it be implemented? 59

6.1 Best option from those considered 59

6.2 Implementation 64

7. How will you evaluate your chosen option against the success metrics? 70

7.1 Approach to evaluation 70

7.2 Indicators of success 71

Appendix A: References to the 2022 RIS 73

Appendix B: Extract of Consultation Paper Questions 77

Appendix C: Consultation Questions & Summary of Industry Views on Draft IA 78

I. Executive summary

The identification and protection of critical infrastructure is essential for Australia's social and economic prosperity, national security, and national defence, and facilitating the provision of essential services. The *Security of Critical Infrastructure Act 2018* (Cth) (SOCI Act), which commenced on 11 July 2018, represented a significant enhancement to Australia's existing regulatory framework at the time. However, the evolving geopolitical and cyber threat environment facing Australia requires regular review of current legal parameters to ensure the security and resilience of critical infrastructure.

The Department of Home Affairs (the Department) remains focused on ensuring the security and resilience of Australia's critical infrastructure, and providing ongoing assurance to the Australian Government that critical infrastructure is being managed in a manner which reflect an inherently complex and evolving risk environment. This includes assessing whether applicable legislation remains fit-for-purpose and engaging with industry to understand and address areas of concern.

The SOCI Act, which seeks to manage national security risks to Australia's critical infrastructure assets, has undergone amendments including through passage of:

- The Security Legislation Amendment (Critical Infrastructure) Act 2021 (SLACI Act). The regulatory impacts of the SLACI Act were considered in a 2020 regulation impact statement (RIS) titled 'Critical Infrastructure, Systems of National Significance' ('the 2020 RIS') (Office of Best Practice Regulation (OBPR) ID: 25902). The 2020 RIS can be accessed here.
- The *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022*) (SLACIP Act). The regulatory impacts of the SLACIP Act were considered in a 2022 RIS titled 'Regulation impact statement: A risk management program framework for critical infrastructure assets' (Office of Impact Analysis (OIA) ID: OBPR22-02914), and hereafter referred to as the '2022 RIS' in this IA. The 2022 RIS can be accessed here.

As part of the 2023-2030 Australian Cyber Security Strategy, the Department consulted with industry on further reforms to the SOCI Act. Between 19 December 2023 and 1 March 2024 the Department held numerous town halls and roundtable discussions with affected entities on potential reforms to the SOCI Act. Industry was also invited to provide written submissions by 1 March 2024 in response to the '2023-2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper' (the Consultation Paper). This IA considers options for implementation more broadly than legislative reforms and considers the regulatory cost of options following industry feedback.

This IA considers the regulatory impacts of the potential SOCI Act reforms through the lens of three problem elements, as outlined in Table 1 below.

Table 1 *Identified problems and Government objectives*

	What is the problem?	What are Government's objectives?
1.1	There are a growing number of cyber incidents which impact non-operational data storage systems held by critical infrastructure entities and can often be a point of entry for malicious actors.	• Ensure **consistent** capture of secondary systems where vulnerabilities could have a relevant impact on critical infrastructure.
1.2	Businesses often face difficulties responding effectively in the aftermath of significant incidents because of legal risks and government's limited ability to support with post-incident consequence management.	• Enable a **coordinated, agile, industry-led response** to incidents with appropriate support from government where necessary.

1.3	When an entity is unwilling to comply with the regulator's recommendations to enhance a risk management program (RMP), there is limited ability for the regulator to issue a direction that the entity remedy the deficient RMP in a timely fashion.	• **Clarify and enhance** the security standards applicable to critical infrastructure. • Enable an **agile, industry-led response** to incidents with appropriate support from government where necessary.

This IA considers three options for addressing the above problem elements:

- **Option 1** – maintaining the status quo (no regulatory change);
- **Option 2** – implementing three reforms to the SOCI Act, including clarification of definitions and introduction of new directions powers; or
- **Option 3** – enhanced collaboration between industry and Government, through use of the Trusted Information Sharing Network (TISN).

A Draft IA consulted on with industry provided an opportunity for industry feedback on the costs and benefits associated with each of these options. Analysis indicates the following in relation to the likely net benefit of each option:

- **Option 1** – maintaining the status quo. This option is not capable of addressing the gaps which have been identified in the SOCI Act, as it involves no change to the Act or broader regulatory environment. Stakeholders will suffer the forgone benefit of consistency, clarity, and agile, industry-led responses in the aftermath of an incident. Critical infrastructure assets will be left more vulnerable to a growing threat of incidents.
- **Option 2** – regulatory change. The likely benefits will be at least (and are expected to be more than) the costs of the regulation. This is primarily because the nature of the reforms means the marginal costs of the proposed changes are expected to be small relative to the benefits of avoided future incidents (which have substantially greater cost). Measures which may attract high costs in some circumstances (such as consequence management) are expected to be used infrequently, mitigating cost impacts. Option 2 allows for achievement of each objective of Government's intervention (outlined in Table 1 above).
- **Option 3** – voluntary engagement from industry via the TISN. Responsible entities who choose not to engage with the TISN will not contribute to improving the current issues which exist in the SOCI Act. Even if there were full engagement across industry, the net benefit is inherently limited because not all required reforms can be addressed through the TISN (given the requirement that directions powers are legislated).

In March 2024, the Department consulted with industry on a draft IA, which invited industry to respond to consultation questions contained in the IA (see Appendix B for the questions included in the draft IA). Consultation asked industry to validate the costs and benefits identified in relation to each option, identify any additional costs and benefits, and (where possible) provide data to support analysis. Insight from this consultation period built on the Department's understanding of industry sentiment gained from submissions on the Consultation Paper.

This IA examines the case for implementing each of the three options described above, and their associated costs and benefits – two of which (Options 2 and 3) demonstrate the potential to achieve some or all of the stated policy objectives, and one which maintains the status quo (Option 1). The analysis presented in this document clearly identifies that **Option 2: Amendments to the SOCI Act** most effectively addresses the identified problem areas, aligns with Government's objectives for consistency, industry-led responses, and enhancement of existing applicable standards. It also offers the greatest overall expected net benefit.

Development of this IA

The Department is engaging closely with the OIA throughout the IA process. This IA is being developed concurrently to key stages in policy development, outlined in Table 2.

Table 2 *Policy development process*

Policy development stage	Relevant IA development stage	Dates
Detailed consultation paper on the nature of the proposed reform measures for industry	Draft IA	19 December 2023 – 1 March 2024
Detailed consultation on the nature of the proposed reform measures to support an Exposure Draft of the Bill (however was unable to be released with the Exposure Draft)	Early Assessment IA	March 2024
Decision by Government to implement proposed reform measures	First Pass IA	July 2024
Final decision by Government to implement proposed reform measures	Second Pass IA	Spring 2024

II. Introduction

A. Purpose of this document

This IA builds on prior reforms to the SOCI Act, considered in regulatory impact analysis conducted in 2020 and 2022. These amendments are summarised below:

- The SLACI Act amended the SOCI Act to apply to additional sectors and introduced additional security requirements including mandatory cyber incident reporting (MCIR) and government assistance measures for critical infrastructure.
- The SLACIP Act amended the SOCI Act to include a framework for a risk management program, declarations of systems of national significance and enhanced cyber security obligations.

Part 2 of the 2023-2030 Australian Cyber Security Strategy Legislative Reforms Consultation Paper introduces five new proposed reforms to the SOCI Act.

This IA analyses the costs and benefits of three new reforms to the SOCI Act:

1. Amendment of definitions in the SOCI Act to ensure capture of systems and networks that hold 'business critical data', where vulnerabilities could have a 'relevant impact' on the asset.
2. Legislating an all-hazards consequence management power, which the Minister may authorise as a last resort, where there is no existing power available to support a fast and effective response.
3. Introduction of a written directions power to compel entities to remedy seriously deficient risk management programs.

The reforms package also includes:

1. Consolidation of security requirements for the telecommunications sector under the SOCI Act.
    - As this is an extension of existing costed obligations to the telecommunications sector, the costs and benefits of this proposal will be separately considered in an Addendum to the 2022 RIS alongside consultation on the relevant instrument.
2. Amendments to clarify the protected information regime under the SOCI Act. These amendments do not produce a regulatory impact.

B. Critical infrastructure in Australia

The Commonwealth Government's Critical Infrastructure Resilience Strategy 2023 defines critical infrastructure as:

> *"…Those physical facilities, systems, assets, supply chains, information technologies and communication networks which, if destroyed, degraded, compromised or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of Australia as a nation or its states or territories, or affect Australia's ability to conduct national defence and ensure national security."*[1]

The Government's ongoing consideration, review, and subsequent amendments to the SOCI Act reflects its priority in ensuring the resilience and protection of Australia's critical infrastructure sectors. Critical infrastructure is vital to Australia's social and economic stability, defence, and national security. It enables the provision of essential services such as food, water, health services, education, energy, communications, transportation, and banking. Without these services, Australia's social and economic prosperity, national security, defence, and public safety would be threatened.

Existing critical infrastructure legislative frameworks are being challenged by an evolving threat environment. Natural hazards are increasing in prevalence, information technology and operational systems are converging, and foreign intelligence activities against Australian national interests are increasing in frequency and sophistication. Recent major cyber security incidents and subsequent

[1] Cyber and Infrastructure Security Centre – Critical Infrastructure Resilience Strategy (pg. 4)

reviews have identified opportunities to clarify and strengthen existing obligations contained in the SOCI Act.

The interconnected nature of critical infrastructure means that, without proper safeguards, deliberate or inadvertent disruption of one critical infrastructure asset can result in cascading consequences. While owners and operators of critical infrastructure have incentives to ensure the resilience of their own assets, the interconnectedness and significance of these assets creates a need for a comprehensive regulatory framework, applied on a sector-agnostic basis.

Operation of the SOCI Act

The SOCI Act is the primary framework for regulation and protection of Australia's critical infrastructure. The Act currently applies to 11 sectors and 22 asset classes (as outlined in Table 3 below), and provides the following key measures for the owners and operators of certain critical infrastructure assets:

- the requirement to report information to the register of critical infrastructure assets, ensuring there is an understanding of Australia's critical infrastructure ecosystem, risks and interdependencies;
- MCIR requirements, ensuring there is a better aggregate understanding of how cyber incidents are impacting Australia's critical infrastructure;
- a requirement to implement and comply with an all-hazards critical infrastructure RMP creating a baseline for security across the critical infrastructure ecosystem. Where certain responsible entities are exempt from the RMP obligation, there are separate applicable annual reporting requirements contained in Part 2AA of the SOCI Act;
- an ability for the Secretary of Home Affairs to impose enhanced cyber security obligations for owners and operators of Australia's most interconnected systems of national significance– working in a close partnership with Government to ensure they are sufficiently prepared and positioned to defend and respond in the event of a significant cyber incident impacting their systems; and
- government assistance measures to help critical infrastructure entities respond to significant cyber incidents as a last resort.

Table 3 *Critical infrastructure sectors and assets*

Critical infrastructure sector	Asset class
Energy	Liquid fuel Gas Energy market operator Electricity
Water and sewerage	Water
Space technology	No asset class
Data storage and processing	Data storage or processing
Communications	Telecommunications Domain name systems Broadcasting
Higher education and research	Education
Defence industry	Defence industry

Critical infrastructure sector	Asset class
Financial Services	Superannuation Insurance Financial markets and infrastructure Banking
Healthcare and medical	Specified critical hospitals
Transport	Aviation Freight infrastructure Freight services Port Public transport
Food and grocery	Food and grocery

1. What is the policy problem you are trying to solve and what data is available?

Following the commencement of the SOCI Act and subsequent amendments, Government and industry have had the opportunity to understand the framework's ability to prevent, manage and respond to incidents in practice. Concurrently, there has been an observed increase in the number of cyber incidents impacting critical infrastructure in Australia. For example:

- In 2023, the **Australian Bureau of Statistics** (ABS) reported that more than two in 10 businesses experienced a cyber security attack during the 2021-22 financial year, an increase from one in ten businesses in 2019-20.[2]
  - 34% of businesses reported loss of time in managing cyber incidents.
  - 18% reported a downtime of service.
  - 17% of businesses reported a loss in staff productivity.
- In 2022-23, the **Australian Signals Directorate** (ASD) responded to 143 incidents reported by entities who self-identified as critical infrastructure, an increase from the 95 incidents reported in 2021-22.[3]
- In 2022-23, 188 mandatory cyber incident reports assessed with a relevant impact were submitted from critical infrastructure entities, under SOCI's **MCIR regime**[4]. These incidents were reported in line with obligations applied to certain critical infrastructure asset classes through the making of rules under the SOCI Act.

The Australian community have expressed a desire for Government to ensure, and demonstrate, that is has the right tools in place to mitigate the occurrence of these incidents and respond quickly in the aftermath of an incident. For example, in the aftermath of the 2022 Optus data breach, a poll by the Guardian found one in two survey participants (from a sample of over one thousand Australians) would support law reform to enhance protections for personal information.[5]

Further, the Cyber and Infrastructure Security Centre's 2023 publication 'Overview of Cyber Security Obligations for Corporate Leaders: Leaders in cyber security governance' identified that:

> "*Many expectations of cyber governance are unclear. Industry feedback has flagged that more could be done to help businesses understand what good cyber security looks like*."[6]

This IA considers three problem elements which currently limit industry and Government's ability to prepare for, prevent and respond to incidents when they occur.

Table 4 *Three problem elements arising from gaps in the SOCI Act*

	Problem elements
1.1	There is a growing number of cyber incidents which impact non-operational data storage systems held by critical infrastructure entities and can often be a point of entry for malicious actors.

[2] https://www.abs.gov.au/media-centre/media-releases/cyber-security-incidents-double-between-2019-20-and-2021-22
[3] https://www.cyber.gov.au/about-us/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023#:~:text=Australian%20critical%20infrastructure%20networks%20regularly,incidents%20reported%20in%202021%E2%80%9322.
[4] https://www.homeaffairs.gov.au/reports-and-pubs/Annualreports/home-affairs-annual-report-2022-23.pdf PG. 264
[5] https://www.theguardian.com/australia-news/2022/oct/04/guardian-essential-poll-one-in-two-australians-want-stronger-privacy-laws-after-optus-breach#:~:text=The%20new%20Guardian%20Essential%20poll,worried%20about%20their%20privacy%20online
[6] https://www.cisc.gov.au/resources-subsite/Documents/overview-cyber-security-obligations-corporate-leaders.pdf PG. 4

1.2	Businesses often face difficulties responding effectively in the aftermath of critical infrastructure incidents because of legal risks and government's limited ability to support with post-incident consequence management.
1.3	When an entity is unwilling to comply with the regulator's recommendations to enhance an RMP, there is limited ability for the regulator to issue a direction that the entity remedy the deficient RMP in a timely fashion.

These gaps demonstrate the need to ensure that critical infrastructure entities apply an all-hazards approach.[7]

While there are a range of legislative frameworks (including the SOCI Act) in place that seek to uplift the security and resilience of critical infrastructure assets, Table 5 below identifies why these regimes are not capable of addressing the problems highlighted above. These gaps have been identified through:

Evaluating the efficacy of existing legislative frameworks (including through Government-led reviews), in light of recent critical infrastructure incidents (such as the Optus and Medibank attacks). These reviews highlighted gaps that limit industry's ability to prepare, prevent and respond to cyber incidents.

- **Review of data related to critical infrastructure incidents.** For example, as mentioned above, the 188 significant or relevant incidents identified through the MCIR in 2022-23 demonstrate opportunities to enhance the legislative frameworks related to the confidentiality, integrity, or reliability of Australian critical infrastructure.
- **Engagement with industry,** including on the Consultation Paper and a draft version of this IA. This consultation has allowed the Department and industry to understand how existing legislative obligations work in practice, including areas of strength and identification of gaps.

[7] 'All-hazards' refers to the primary objective of Australia's critical infrastructure regulation, to improve critical infrastructure resilience and mitigate the potential impacts of natural and physical hazards (for example, fires, floods and cyclones, health hazards) and hazards related to cyber, personnel and supply chains (for example, unlawful interference, cyber incidents, espionage, chemical or oil spills, and trusted insiders). 'All-hazards' and the corresponding hazard domains were analysed in further detail in the Regulation impact statement: a risk management program framework for critical infrastructure assets (pp. 18 – 19).

Table 5 *Overview of existing Commonwealth critical infrastructure legislation*

Overview of existing regulation		Identified gap
Security of Critical Infrastructure Act 2018 **(Cth)**	Establishes a framework for managing risks to national security related to 'critical infrastructure assets' by, among other mechanisms, creating a Register of Critical Infrastructure Assets.	In considering all current SOCI Act obligations, the Department and industry have had the opportunity to engage with and observe the operation of these obligations in practice. This includes the framework's interaction with the various operating environments of each critical infrastructure asset, the application of other Australian legislative regimes and initial observations on industry education and compliance exercises. While the SOCI Act works to uplift and maintain all-hazards risk management, recent incidents in Australia have highlighted gaps in the regime's operation. These include lack of clarity in definition and gaps in enforcement powers, which are not currently contained in the Act.
Security Legislation Amendment (Critical Infrastructure) Act 2021 **(Cth)**	Established an enhanced framework for managing cybersecurity risks to an expanded list of 'critical infrastructure assets' by, among other mechanisms, including MCIR and Government Assistance powers.	In considering all current SOCI Act obligations, the Department and industry have had the opportunity to engage with and observe the operation of these obligations in practice. This includes the framework's interaction with the various operating environments of each critical infrastructure asset, the application of other Australian legislative regimes and initial observations on industry education and compliance exercises. While the SOCI Act works to uplift and maintain all-hazards risk management, recent incidents in Australia have highlighted gaps in the regime's operation. These include lack of clarity in definition and gaps in enforcement powers, which are not currently contained in the Act.

Overview of existing regulation		Identified gap
Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 **(Cth)**	Introduced critical infrastructure risk management program obligations to require all hazards risk management for certain assets. Established the ability to designate the most important critical infrastructure assets as systems of national significance and apply enhanced cyber security obligations to these assets.	In considering all current SOCI Act obligations, the Department and industry have had the opportunity to engage with and observe the operation of these obligations in practice. This includes the framework's interaction with the various operating environments of each critical infrastructure asset, the application of other Australian legislative regimes and initial observations on industry education and compliance exercises. While the SOCI Act works to uplift and maintain all-hazards risk management, recent incidents in Australia have highlighted gaps in the regime's operation. These include lack of clarity in definition and gaps in enforcement powers, which are not currently contained in the Act.
Foreign Acquisitions and Takeovers Act 1975 **(Cth) ('FATA')**	Sets out the circumstances and processes for decision making in relation to foreign investment applications - known as 'significant actions'. Under the FATA, the Treasurer (in consultation with other relevant bodies) may allow the action, impose conditions on the action, prohibit the action, or require that the action be undone.	The FATA is not designed to directly consider the risk management activities of Australia's critical infrastructure and cannot address the identified gaps. Any amendments to the SOCI Act will complement the operation of the FATA.
Privacy Act 1988 **(Cth)**	Promotes the protection of individuals' privacy and provides regulations through 13 Australian Privacy Principles (APPs) for public and private APP entities with an annual turnover greater than 3 million dollars in relation to how personal information is handled.	The Privacy Act will remain the primary lever for the protection of personal information, given its unique ability to regulate the large-scale collection and distribution of data. While personal privacy remains a key focus of the Privacy Act, business critical data in SOCI is necessarily extended to consider data relevant to the reliability, availability, confidentiality and integrity of an asset such as operational or research data.

Overview of existing regulation		Identified gap
Aviation Transport Security Act 2004 **('ATSA')**	Establishes mechanisms to safeguard interference with aviation. The Act outlines ways in which the aviation industry must implement Transport Security Programs to set out how participants will manage security for their operations, as well as establishing reporting obligations in relation to any deemed aviation security incidents.	The ATSA and MTOFSA do not currently impose an all-hazards approach to risk management. There is also no equivalent consequence management power in these Acts.
Maritime Transport and Offshore Facilities Security Act 2003 **('MTOFSA')**	Provides safeguards against interference with maritime transport or offshore facilities. Establishes a regulatory framework to develop and implement a security plan for ships, other maritime transport operations and offshore facilities to successfully achieve maritime security outcomes.	The ATSA and MTOFSA do not currently impose an all-hazards approach to risk management. There is also no equivalent consequence management power in these Acts.
Part 14 of the ***Telecommunications Act 1997***	Establishes a regulatory framework for the security of telecommunications entities including carriers and service providers.	The SOCI Act is currently limited in its application to the telecommunication sector. Any potential amendments to the SOCI Act will work to contribute to a clear single regulatory framework for the security of telecommunications assets to address legislative complexities in security and risk mitigation for the sector.
National Emergency Declaration Act 2020 **('NED')**	The Governor-General may make a declaration, called a national emergency declaration, on the advice of the Prime Minister, in circumstances where an event is causing harm that is nationally significant in Australia or in an Australian offshore area. In such instances, the declaration may cause certain provisions of Commonwealth laws to be modified including requirement of Government Departments to provide information to assist in preparing for, responding to or recovering from the emergency.	The NED Act does not specifically address disruptions to critical infrastructure nor provide an avenue to support industry to manage national security risks in the aftermath of a critical infrastructure incident. Any potential amendments to the SOCI Act will complement the framework contained in the NED Act and streamline the exercise of existing national emergency powers.

The legislative mechanisms and gaps highlighted above demonstrate the need for consistent consideration, and where appropriate, amendment of legislation, to mitigate risks arising from vulnerabilities in highly interconnected sectors. This is not unexpected, as observing the operation of and engaging with legislation in practice and in light of recent major cyber incidents, provides insights on how these instruments can capture and address all necessary circumstances.

1.1 Growing number of cyber incidents which impact non-operational data storage systems held by critical infrastructure entities.

Cyber incidents in Australia are increasing in frequency and complexity. The ASD's analysis of Australia's cyber threat landscape in 2022-23 identified critical infrastructure as a key target of malicious state and non-state cyber actors. The ASD's Annual Cyber Threat Report states:

> "*Australian critical infrastructure was targeted via increasingly interconnected systems. Operational technology connected to the internet and into corporate networks has provided opportunities for malicious cyber actors to attack these systems.*"[8]

The 2023-2030 Australian Cyber Security Strategy similarly identifies the need for a continued focus on critical infrastructure resilience:

> *"…in the face of heightened geopolitical risk, capable nation-state actors, and sophisticated cybercriminals. Cyber incidents affecting critical infrastructure entities may cause cascading impacts across the Australian economy due to our heavy reliance on their services."*[9]

The following case studies are two significant examples of cyber-attacks which have recently occurred in Australia and demonstrate a clear imperative for decisive action to prevent the occurrence of similar future incidents.

Table 6 *Overview of Medibank Cyber Incident*

Medibank Cyber Incident (Cyber)
Situation: On 13 October 2022, Medibank, an Australian medical insurer, detected unusual activity on its internal systems. Medibank commenced an investigation into the activity, initially believing there was no evidence that any customer data had been compromised. However, Medibank was contacted by a hacker who claimed to have stolen 200GB of past and present customer data and threatened to release the information onto the dark web. After Medibank refused to pay a ransom, the hacker began releasing sensitive customer files on the dark web.[10] The Australian Federal Police identified the hackers as being linked to a Russian hacking group.[11] It was determined the hackers were able to infiltrate the network through use of a stolen username and password used by a third-party IT service provider.[12] The hackers then accessed Medibank's network via a 'misconfigured' firewall, which did not require an additional digital certificate.[13]

[8] ASD, https://www.cyber.gov.au/sites/default/files/2023-11/asd-cyber-threat-report-2023.pdf pg. 1
[9] https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf pg. 41
[10] https://www.medibank.com.au/livebetter/newsroom/post/medibank-cybercrime-update%207%20November
[11] https://www.medibank.com.au/livebetter/newsroom/post/statement-by-afp-commissioner-reece-kershaw-on-medibank-private-data-breach
[12] https://www.medibank.com.au/content/dam/retail/about-assets/pdfs/investor-centre/results/HY23_Results_Media_Release.pdf PG. 5
[13] https://www.medibank.com.au/content/dam/retail/about-assets/pdfs/investor-centre/results/HY23_Results_Media_Release.pdf PG. 5

Outcome: In the attack, 9.7 million records were stolen, including names, dates of birth, Medicare numbers, and sensitive medical information.[14] In a statement on its 2023 half-year results, Medibank indicated it continued to defend around 18 million perimeter cyber incidents per day.[15]

In February 2023, Medibank reported a loss of almost 13,000 policy holders in the December quarter.[16] Notably, these figures do not contemplate the potential costs of forgone new customers, who may have chosen another policy provider given the reputational damage to Medibank. The company has reported it spent more than $26 million in strengthening its cyber defences between October 2022 and December 2022.[17]

Table 7 *Overview of Optus Data Breach*

Optus Data Breach (Cyber)
Situation: On 22 September 2022, Optus experienced a data breach that led to the unauthorised accessing of details for 11 million customers. The information accessed included customer names, dates of birth, phone numbers, email addresses, home addresses, driver's licence and passport details, and Medicare ID numbers. The breach reportedly occurred as the result of a hacker accessing an 'unauthenticated API endpoint', meaning there was no requirement to 'log in'. The hacker demanded that Optus pay them US$1 million ransom, or data of the 11 million affected customers would be published. The hacker then posted a text file of 10,000 customer data records on September 26, allowing other malicious actors to use the data in their own phishing campaigns. Victims of the breach reported on September 27 that they had been contacted with demands that they pay AU$2,000 or their data will be sold to other hackers.
Outcome: Optus has indicated the company will incur costs of up to AU$142 million as a result of the data breach, including the cost of commissioning an independent report into the incident by Deloitte.[18]

These incidents highlight the need to ensure critical infrastructure entities have adequate protections in place across non-operational data storage systems. While the existing SOCI Act framework includes requirements for risk management activities for data storage, the current definition of 'critical asset' does not include secondary systems.

While the above scenarios did not impact the provision of essential services, the following hypothetical scenarios further demonstrate where the existing regulatory framework applies inconsistent data protections, leaving obligations subject to the interpretation of individual entities.

[14] https://www.foreignminister.gov.au/minister/penny-wong/media-release/cyber-sanctions-response-medibank-private-cyber-attack; https://www.medibank.com.au/livebetter/newsroom/post/medibank-cybercrime-update%207%20November

[15] https://www.medibank.com.au/content/dam/retail/about-assets/pdfs/investor-centre/results/HY23_Results_Media_Release.pdf PG. 5

[16] https://www.medibank.com.au/livebetter/newsroom/post/2023-half-year-results-a-solid-result-with-business-momentum-returning

[17] https://www.medibank.com.au/livebetter/newsroom/post/2023-half-year-results-a-solid-result-with-business-momentum-returning

[18] https://www.optus.com.au/content/dam/optus/documents/about-us/media-centre/financial-reports/2022/halfyear_optus.pdf PG. 2; https://www.optus.com.au/content/dam/optus/documents/for-you/support/cyberattack/cyber_incident_letter_251022.pdf PG. 2

Table 8 *Hypothetical Scenario – Storage of operational data*

Storage of operational data (Hypothetical scenario)
Scenario: A major port has operational data stored with a third-party data storage or processing provider (which is regulated under the SOCI Act).
Outcome: Under current legislative obligations, the data storage and processing entity contracted by the major port has obligations under the SOCI Act to protect the system that holds business critical data. If a breach occurred in this system, the data storage and processing entity has an existing obligation to report any data breaches under the MCIR in the SOCI Act. The requirements applicable to the third party, including a reporting obligation, are clear and contribute to an enhanced ability for industry and Government to respond.

Table 9 *Hypothetical Scenario – Storage of customer data*

Storage of customer data (Hypothetical scenario)
Scenario: A specified critical hospital has patient data stored within a data storage system to assist with the operations of the intensive care unit (which forms part of their existing critical infrastructure asset).
Outcome: If the data storage system was subject to an eligible data breach, the hospital would have an obligation under the Privacy Act to report the breach to affected persons and the Australian Information Commissioner. However, the format and application of the regulatory framework applicable to the designated hospital mean it is unclear whether the hospital should consider business critical data as part of their existing risk management obligations or report it under the MCIR obligation. An inability to access patient data may impact on the provision of essential services.

Consultation with industry has highlighted issues which arise from ambiguities in the scope and obligations of businesses under the Act, including in relation to business critical data.

Any requirements to capture secondary systems as part of risk management activities will be specifically designed to reduce the likelihood and severity of incidents of the kind described above and seek to address industry views on the ambiguities which arise under the existing regime.

1.2 Businesses face difficulties responding effectively in the aftermath of an incident

All-hazards incidents have significant ongoing effects beyond the affected entity. Cyber incidents may result in significant harms to individuals, organisations, and businesses, such as theft of sensitive data, substantial financial loses, reputational damage and loss of consumer confidence, as well as across the wider economy.

While most critical infrastructure entities are willing to address the consequences of incidents impacting their assets, there can be legal or other restrictions which inhibit their ability to do so effectively and efficiently. Government reviews in the aftermath of the Optus and Medibank incidents (described above) highlighted the lack of a clear power to support in the aftermath of an incident. Legal restrictions meant entities were not permitted to share information about affected customers to banks, in an effort to prevent financial fraud. Government was also without a legal power to direct entities to share this information.

There are some legislative powers in place, in the SOCI Act and beyond, which may allow Government to intervene where there are risks to critical infrastructure assets. However, these powers do not currently extend to consequence management, as described in Table 10 below.

Table 10 *Gaps in existing legislation for consequence management*

	Overview of existing regulation	Identified gap
Security of Critical Infrastructure Act 2018 **(Cth)**	Part 3A contains government assistance measures which are designed to assist with the immediate response to serious cyber security incidents, where they pose a material risk to Australia's national interests. The powers allow Government to support in defending critical infrastructure from incidents which may impact delivery of essential services.	The powers in Part 3A cannot be used for consequence management because they are limited in scope to the incident itself, not the consequences following an incident's occurrence. The powers are not designed to manage secondary consequences, no matter the severity or scale of impact. It is the responsibility of critical infrastructure owners and operators to consider and plan for these risks and implement appropriate strategies to manage incidents impacting their assets. Further, Part 3A may only be used when a cyber-origin has been established (rather than, for example, a natural hazard or personnel hazard) – something often difficult to achieve in a high intensity, time critical environment.
National Emergency Declaration Act 2020 **(Cth)**	Enables the Governor-General to make a national emergency declaration on the advice of the Prime Minister. It also allows a responsible Commonwealth Minister to streamline the exercise of existing national emergency powers listed in the NED Act.	While the NED Act is designed to reduce red tape and the administrative burden of people affected by a national disaster, it does not specifically address consequence management in the aftermath of an incident. The NED Act and the ability for the Minister to streamline the exercise of existing national emergency powers (which includes part 3A of SOCI) could be used in tandem with amendments to enhance overall incident response.

These gaps can have tangible impacts on timely incident management and recovery. This also directly effects the financial costs which might arise from an all-hazards incident, including costs to an individual, the affected entity, and the Australian economy. The hypothetical scenarios set out below further demonstrate how the identified gaps in the existing legislative framework may affect industry and Government in practice.

Table 11 *Hypothetical Scenario – Research data stolen from a university*

Research data stolen from a university (Hypothetical scenario)
Scenario: As part of ongoing efforts to utilise Australian expertise for socioeconomic coercion, confidential research data could be stolen by compromising university research databases. Once stolen, this data could be used by state-based attackers to undermine other critical infrastructure systems. Malicious actors could use the stolen data to plan widespread attacks on critical services and cause disruption to functions of other critical infrastructure assets. While the university could investigate the

incident and upgrade their cyber defences, the Government is uniquely placed to address the consequences for other critical infrastructure entities whose security could be impacted by the stolen data. The university may be unable to act as it does not have access to national communication channels or the asset register.

Outcome: In this scenario, current government assistance powers would only allow the Government to issue directions in relation to the technical cyber incident. A new consequence management power would be needed to issue directions to certain other critical infrastructure entities whose systems and critical functions have or will be disrupted due to the data breach. These directions could include directing those specific entities to upgrade information technology (IT) and operational technology (OT) security to address system vulnerabilities. If compliance with these directions would risk breaching existing contracts with IT and OT service providers, critical infrastructure entities would be able to rely on the SOCI Act's immunity provisions to avoid civil liability for such breaches.

Table 12 *Hypothetical Scenario – Disruptions caused from non-cyber hazards*

Disruptions caused from non-cyber hazards (Hypothetical scenario)
Scenario: It is the middle of summer and energy generation is already operating near peak capacity. A malicious insider and issues-motived actor sabotages a gas pipeline near agricultural land, causing an uncontrolled release of gas and liquid fuels that results in cessation of gas to a large population. The critical infrastructure gas supplier is willing to cease the flow of gas to reduce physical hazards but cannot coordinate the delivery of gas from other sources, nor can it adequately address all health hazards caused by land contamination.
Outcome: In this scenario, the Government may need to issue a 'do not disturb' / quarantine order for the contaminated area and, if the entity is unable or unwilling to cooperate, direct the entity to allow emergency access to sensitive land for decontamination efforts. Concurrently, the Government may need to coordinate alternate transport of critical liquid fuels to support the operation of other critical infrastructure sectors. Finally, the Government may need to redirect resources and issue prioritisation orders for electricity supply to households and hospitals if energy demand outstrips generation supply that may otherwise be supplemented by gas-powered redundancy. However, the current legislative framework (with no directions power available) limits Government's ability to undertake actions of this kind.

Engagement with industry remains a key focus for the Department. The Department recognises that addressing these concerns requires flexibility and acknowledgement of the potentially significant flow-on impacts of an all-hazards incident, such as a cyber incident or natural disaster.

1.3 No ability for the regulator to issue a direction to an entity to remedy a deficient RMP

Since the SOCI Act's introduction and its subsequent amendments, the Cyber and Infrastructure Security Centre (CISC) and the Department have worked to support responsible entities, using the following principles:

- **Promotion of voluntary compliance** through effective engagement with industry and its regulators, with clear guidance on legislative requirements and how to comply.
- **Evidence-based compliance and enforcement actions** that respond to the nature and seriousness of non-compliance and potential security risks to Australian critical infrastructure.
- **Commitment to an industry and Government partnership**. Through the Trusted Information Sharing Network (TISN) the Department works closely with industry and other government bodies to share threat information and risk advisories with Australia's critical infrastructure and works collaboratively to collectively uplift the security and resilience of Australia's critical infrastructure.

- **Commitment to transparency and reporting on compliance action**. The SOCI Act requires the Minister to table an annual report to Parliament, affording greater oversight to any decision or action taken under the SOCI Act or the regulations.
- **Integrity, professionalism and procedural fairness to compliance and enforcement**. Compliance, monitoring, and enforcement activities will be undertaken with integrity, professionalism and with due regard to procedural fairness, privacy, and information sensitivity.

These principles are complemented by a suite of existing regulatory options under the SOCI Act designed to address non-compliance. The specific legislative power, as well as the identified gap in its current application, is outlined in Table 13 below.

Table 13 *Gaps in existing legislation*

	Overview of existing regulation	Identified gap
Security of Critical Infrastructure Act 2018 **(Cth)**	Section 37 of the SOCI Act permits the Secretary of Home Affairs to require that an entity produce any document that is relevant to compliance with the Act or determining whether a power should be exercised, which may include its RMP.	When an entity fails to maintain adequate risk preparedness and mitigation in their RMP, they cannot be directed to take specific actions to improve their RMP or other risk management related practice without an enforceable undertaking being sought (see below discussion of enforceable undertakings). This represents a gap in the graduated regulatory powers available to the regulator.

The identified gap above makes it challenging for the SOCI Act to achieve its intent of embedding preparation, prevention, and mitigation activities into the business-as-usual operations. The CISC is currently undertaking trial audits of critical infrastructure entity compliance with SOCI Act obligations. Early findings are that a significant proportion of entities are not fully compliant with the existing CIRMP obligation, which suggests there will be a need for appropriate intervention powers to ensure compliance and effective risk mitigation. The full extent of this level of non-compliance is yet to be established.

Under the status quo, the Department is limited to pursuing an enforceable undertaking when compelling an entity to address deficient risk management practices in the following example:

- Where the entity is not meeting or taking reasonable steps to meet required maturity levels of prescribed cyber security frameworks;
- Where an entity does not have a process in place to assess the suitability of critical workers that have access to critical components of a critical infrastructure asset; and
- Where the entity has failed to consider and minimise risks in the threat landscape that pose a potential risk to their asset, the Secretary may direct the entity to consider those risks. For example, if an electricity distributor has failed to minimise the threat posed by cyber-attacks on their operational technology.

While an enforceable undertaking offers some avenue for recourse where there is a deficient RMP, there are substantial costs and lead times, for both entities and the Department, associated with attaining an undertaking, due to the procedural matters it involves. An enforceable undertaking also removes the discretion which may be desirable when an entity is considering how to respond to a direction to address a deficient RMP.

In addition, an enforceable undertaking:

- Cannot be compelled by the Department. It instead relies on the entity providing a written undertaking to the Department.

- Is unlikely to be provided by an entity with a deficient RMP and therefore, cannot be enforced by the Department.

When an entity makes an enforceable undertaking and later fails to comply, the process of enforcement creates additional time and cost burdens. This is because:

1. The Department may first seek to resolve the matter through consultation in appropriate cases, which is a time consuming process for both the Department and relevant entity.
2. Where consultation is not appropriate or where no resolution is possible, the Department may proceed to apply to the Federal Court to make appropriate orders to enforce the terms of the undertaking. The procedural matters involved in seeking appropriate orders, including delays in court proceedings, will also add additional time and cost burdens.
3. In the course of seeking to enforce the undertaking, risks arising from the deficient RMP may have already materialised, creating potential harms for industry and Australia at large.

2. What are the objectives, why is government intervention needed to achieve them, and how will success be measured?

2.1 What are the objectives?

There are several specific objectives for Government intervention, aligned with the three problem elements identified in Section 1. These are outlined in the Table 14 below.

Table 14 *Identified problems and Government objectives*

	What is the problem?	What are Government's objectives?
1.1	There is a growing number of cyber incidents which impact non-operational data storage systems held by critical infrastructure entities, which can often be a point of entry for malicious actors.	Ensure **consistent** capture of secondary systems where vulnerabilities could have a relevant impact on critical infrastructure.
1.2	Businesses often face difficulties responding effectively in the aftermath of significant incidents because of legal risks and government's limited ability to support with post-incident consequence management.	Enable a **coordinated, agile, industry-led response** to incidents with appropriate support from government where necessary.
1.3	When an entity is unwilling to comply with the regulator's recommendations to enhance an RMP, there is limited ability for the regulator to issue a direction that the entity remedy the deficient RMP in a timely fashion.	**Clarify and enhance** the security standards applicable to critical infrastructure. Enable an **agile, industry-led response** to incidents with appropriate support from government where necessary.

The justification for Government intervention to achieve these objectives, as well as measures of success, are discussed throughout this section.

There may be some barriers to Government achieving the objectives outlined above, including:

- **Governance and policy barriers**, including processes and procedures which may be required to precede both Government intervention and commencement of Government action
- **Resource barriers**, including financial and personnel challenges for responsible entities, which may impede Government's ability to quickly take action to achieve its objectives.
- **Stakeholder environment barriers**. While Government is committed to an ongoing, genuine dialogue with industry and relations are strong, a potential lack of trust from industry stakeholders may limit industry's willingness to collaborate with Government on critical infrastructure matters.

2.2 Why should Government intervene?

Section 1 has highlighted gaps in the existing regulatory framework which may leave Australia's critical infrastructure vulnerable in a rapidly changing risk environment. There is direct alignment between these identified gaps and Government's objectives for the regulation of critical infrastructure, as identified in the Table 14 above.

To achieve these objectives, Government should intervene because:

1. **Government maintains a unique ability to regulate across sectors**;

2. **Government already holds primary responsibility for regulating Australia's critical infrastructure**[19] including, where possible, working in partnership with industry to ensure regulated entities understand and manage their own risk; and
3. **Government can use its convening power to support industry responses and oversight to intervene** (where necessary) to ensure vulnerabilities in critical infrastructure assets are proactively detected, prevented, and resolved.

While self-regulation by industry has been considered as an alternative to government action, the nature of Australia's critical infrastructure sectors mean it is not a viable option in this case. This is because:

- In order to be effective, regulation of critical infrastructure (including regulatory standards and the extent to which risks must be mitigated and managed) must be consistent across all sectors.
- Self-regulation by industry may lead to inconsistent approaches to risk management and therefore varying levels of resilience across Australia's critical infrastructure.
- The nature of the reforms analysed in this IA relate to amendments to an existing ecosystem of regulation, which involves (and relies on) Government intervention. This includes the crucial ability of Government to identify and correct severe deficiencies in industry's approach to risk management.
- Therefore, ongoing Government intervention through Government's whole-of-sector remit, can effectively mitigate the potential impacts of disruption on Australia's social and economic stability, defence, and national security.

Despite the need for Government intervention, the Department prioritises cooperation with industry to support optimal outcomes. This includes, for example, recognising that industry is best placed to assess specific risks, alongside Government who (as regulator) prescribes a baseline level of risk management and accountability.

In order to support industry and operate effectively in the current threat environment, Government must be equipped with the right tools to enable preparation, prevention, and recovery in the event of an all-hazards incident. This threat environment gives rise to a need for Government to intervene to ensure:

- **Clarity:** The security standards of critical infrastructure need to be clarified and enhanced, particularly within the telecommunications sector;
- **Consistency:** The application of the SOCI Act needs to consistently capture the secondary systems where vulnerabilities could have a relevant impact on critical infrastructure; and
- **Coordination:** The SOCI Act needs to enable an agile, industry-led response to incidents with appropriate support from government when necessary.[20]

Government has, and continues to, prioritise close consultation (and where possible, co-design) with industry on any proposed reforms to the critical infrastructure regulatory environment. This has included:

- Previous consultation on the SLACI Act and the SLACIP Act, including publication of a consultation paper, acceptance of submissions and conversations with more than 2,000 industry participants.

---

[19] The 2020 RIS, which can be accessed here, considered enhancements to the SOCI Act including positive security obligations, enhanced cyber security obligations, government assistance and ministerial directions measures. Subsequently, the 2022 RIS, which can be accessed here, introduced risk management program obligations for captured critical asset classes which is overseen by the Department.

[20] *2023–2030 Australian Cyber Security Strategy: Legislative Reforms | CONSULTATION PAPER (homeaffairs.gov.au) (pg. 34).

- Consultation on and co-design of the Critical Infrastructure Risk Management Program (CIRMP rules), through several sector-agnostic town halls, sector-specific workshops, and sector-specific information sessions.
- Co-design included collaboration between Government and industry to agree on key items for codification through rules. This also included the collection of data from industry to support quantification of the costs associated with RMP compliance.
    - Formal consultation on the CIRMP rules was undertaken for a 45 day period and included acceptance of submissions and conversations with industry participants.

Through consultation, Government gathered feedback to actively understand stakeholder concerns, seeking to address these through refinements to regulatory proposals. For example, in consulting on the positive security obligations (PSOs) now contained in the SOCI Act, stakeholders expressed their concerns on the potential for duplication of existing regulatory frameworks. In response, Government developed 'on switches' for PSOs, to ensure obligations were only imposed in cases where there is no existing, comparable regulatory framework.

For details on Government's approach to consultation on the current reform package, see section 5.

Government's established mechanisms for industry engagement and cooperation, focused on ensuring all-hazard risks are appropriately managed, continue to support the case for Government's ongoing intervention:

- **The Critical Infrastructure Resilience Strategy** (the CIRS) provides a national framework for guiding Australia to enhanced critical infrastructure security and resilience. The CIRS includes an overarching vision for critical infrastructure, the impacts of changes in operating environments on critical infrastructure, and points of alignment between the Strategy and existing work across government, to enable achievement of objectives.[21]
- **The TISN** is Government's primary tool for business-government information sharing and resilience-building initiatives on critical infrastructure. The TISN provides a platform for industry and government representatives to share information that enhances mutual understanding and application of organisational resilience and contribute to achievement of the CIRS.[22]
- **The CISC** is responsible for regulating the existing all-hazards critical infrastructure regime, indicates Government's commitment to working with asset owners and operators through engagement, partnerships, advice, exercises, modelling and regulation.[23]

In addition, Government's continued involvement with critical infrastructure matters through review and amendment of the applicable regulatory regime, aligns with each of the key objectives in the CIRS, including to:

- Support critical infrastructure owners and operators to effectively manage risks to the continuity of their operations through mature risk-based and resilient approaches.
- Deliver initiatives through strong industry-government partnerships.
- Support critical infrastructure owners and operators to strengthen their security and resilience through regulatory frameworks, tools, and improved collaboration.

2.3 How will success be measured?

Measuring the success of Government's intervention and the broader reform package will allow the Government to identify and communicate to the Australian community on its chosen regulatory approach. This includes clearly articulating the linkages between the SOCI regime, Government's objectives for intervention, and the relevant measure of success (as outlined in the table below). The

[21] https://www.cisc.gov.au/how-we-support-industry/organisational-resilience/critical-infrastructure-resilience-strategy
[22] https://www.cisc.gov.au/how-we-support-industry/partnership-and-collaboration/trusted-information-sharing-network
[23] https://www.cisc.gov.au/about-us

indicators and evidence of success outlined below will also underpin evaluation of the chosen option in IA Question 7, to ensure these linkages are prioritised in the implementation and evaluation stages.

Table 15 *Identified problems and Government objectives*

Government objectives	Indicator of success	Evidence of Success
Ensure **consistent** capture of secondary systems where vulnerabilities could have a relevant impact on critical infrastructure.	All relevant secondary systems are captured by regulation, reducing the risk of adverse impacts on critical infrastructure.	Industry reporting on approaches to risk management for secondary systems. Specifically: • A stronger understanding of the need to capture secondary systems and the indicators of malicious attacks; and • A reduction in the number of (or severity of) critical infrastructure attacks arising through secondary systems.
Enable a **coordinated, agile, industry-led response** to incidents with appropriate support from government where necessary.	Industry are equipped and informed to deal with incidents, including when to seek Government support.	Industry reporting on approaches to incident response management. Specifically: • A stronger understanding of the ways in which industry can best respond; and • A flexible and transparent approach to interactions with Government, including leveraging Government support at appropriate points.
Clarify and enhance the security standards applicable to critical infrastructure.	Industry have a clear view on applicable standards.	Industry reporting on applicable standards. Specifically: • An ability to clearly identify, implement and comply with standards applicable to their relevant asset.

Consideration of these objectives and measures of success has supported the development of options.

3. What policy options are you considering?

Three options are being considered in response to the identified problem elements:

- **Option 1:** Maintain the status quo.
- **Option 2:** Amend the SOCI Act to**:**
  - Ensure capture of systems holding 'business critical data', where vulnerabilities could have a 'relevant impact' on the asset, in relevant definitions in the Act and RMP rules as required.
  - Legislate an all-hazards power, which may be authorised by the Minister as a last resort, where there is no existing power available to support a fast and effective response.
  - Introduce a formal, written directions power to address seriously deficient RMPs.
- **Option 3:** Enhance collaboration with industry, through use of the TISN, to support industry in filling the gaps identified in Section 1, on a voluntary basis.

Each option is described in detail below, including implementation considerations as applicable.

Development of options

Options analysed in this IA have been developed with reference to the following:

- **Ongoing monitoring and evaluation of the existing regulatory framework**, in order to identify gaps and consider mechanisms (regulatory or otherwise) which may be capable of filling these gaps. Mechanisms such as the TISN allow Government to be informed by industry's views of current and emerging threats, including areas where legislative frameworks can be strengthened.
- **Consistent engagement with industry,** to enhance Government's understanding of how existing regulatory frameworks are operating in practice, and industry's level of understanding of these frameworks. This has allowed for identification of areas where legislation can be clarified or simplified.
- **Consideration of how other governments have responded to critical infrastructure risks.** For example, the United Kingdom's (UK) National Cyber Security Centre has similarly identified an 'enduring and significant' threat to critical infrastructure, requiring the UK Government to consider acceleration of critical infrastructure-related regulatory matters.[24]

In addition to the above considerations, options have been formulated to reflect a range of viable proposals which consider both non-regulatory and regulatory courses of action, with reference to the need to limit (where possible) the regulatory burden on industry.

3.1 Option 1: Maintain the status quo

Option 1 involves no regulatory action or legislative change to the SOCI Act or broader regime. Existing legislation, regulations, standards, guidelines, industry engagement strategies, including through the TISN and CISC social media channels relating to critical infrastructure would remain.

Section 1 of this IA describes status quo regulatory arrangements and the identified gaps in these arrangements. If Option 1 were pursued, the problems identified in Section 1 and described in Table 16 below would persist.

Table 16 *Impact of inaction under the status quo*

Status Quo Arrangement	Impact of Inaction
There is a growing number of cyber incidents which impact non-operational data storage systems held by critical infrastructure entities and can often be a point of entry for malicious actors.	Under the status quo, no action would be taken to ensure these systems are adequately protected. This means cyber incidents may arise on an increasing basis, including through intervention of malicious actors, impacting on the

[24] https://www.ncsc.gov.uk/news/ncsc-warns-enduring-significant-threat-to-uks-critical-infrastructure

	stability of critical infrastructure data and leading to the compromise of sensitive data.
Business often face difficulties responding effectively in the aftermath of critical infrastructure incidents because of legal risks and government's limited ability to support with post-incident consequence management.	Under the status quo, no action would be taken to enhance government's ability to support industry in the aftermath of an incident. This means the time and cost burdens associated with an incident will continue to be borne by industry, with flow on effects to critical services used, and relied upon, by Australians.
When an entity is unwilling to comply with the regulator's recommendations to enhance an RMP, there is limited ability for the regulator to issue a direction that the entity remedy the deficient RMP in a timely fashion.	Under the status quo, this limited ability to intervene through a direction would continue. This means that there is an ongoing risk that vulnerabilities arising from a deficient RMP will materialise, with potentially significant impacts (costs, data compromise and service disruption) for the relevant entities and Australia as a whole.

As described in the table above, under Option 1, current risks arising from the existing threat environment would continue to exist and possibly increase. These risks have manifested in the realisation of significant incidents, such as the Optus and Medibank data breaches. Where no action is taken to address these risks, there is an ongoing threat of these occurrences, with widespread (or potentially more severe) impacts. Similarly, smaller scale incidents may occur more frequently, with impacts accumulating to industry, individuals, and government over time.

3.2 Option 2: Amend the SOCI Act

Option 2 involves three reform measures to the SOCI Act which would require mandatory compliance from industry. Option 2 does not contemplate capture of any additional critical infrastructure sectors or assets beyond those currently required to comply with the SOCI Act. However, existing industry engagement strategies, including through the TISN and CISC social media channels relating to critical infrastructure would remain.

3.2.1 Measure 1: Protecting Critical Infrastructure – Data systems and business critical data

Measure 1 involves amendment to two definitions:

- The definition of all critical infrastructure assets in the SOCI Act; and
- The definition of 'material risk' in s 6 of the CIRMP rules and other sector-specific RMPs.

The practical implications of these changes are described in the hypothetical scenario below.

Table 17 *Hypothetical scenario - operation of Measure 1*

Storage of customer data (Hypothetical scenario)
Scenario: A specified critical hospital has patient data stored within a data storage system to assist with the operations of the intensive care unit (which forms part of their existing critical infrastructure asset).
Current Outcome: If the data storage system was subject to an eligible data breach, the hospital would have an obligation under the Privacy Act to report the breach to affected persons and the Australian Information Commissioner. However, the format and application of the regulatory framework applicable to the designated hospital mean it is unclear whether the hospital should consider business critical data as part of their existing risk management obligations or report it under the MCIR obligation. An inability to access patient data may impact on the provision of essential services.

Operation of Measure 1: If Measure 1 is implemented, the hospital would have an obligation to include the patient data storage system in its all-hazards risk mitigation activities. This requirement may reduce the risk of a data breach in the first instance. It would also provide clarity for the hospital that, depending on the nature of the breach, reporting under the MCIR obligation would apply. This would allow for relevant incident recovery activities to take place, limiting the impact on the provision of essential hospital services.

The proposed definitional changes are described in further detail below.

Asset definition

The amendment would see the inclusion of certain data storage systems which hold 'business critical data' in the definition of all critical infrastructure assets in the SOCI Act. This amendment would:

- Mandate that all asset classes consider data storage systems which hold 'business critical data' as part of their broader critical infrastructure asset, where vulnerabilities in these systems could have a 'relevant impact' on critical infrastructure.
- Enable business critical data storage systems to be considered as an asset by other relevant definitions in the SOCI Act, including the definition of an explicit material risk under the CIRMP (see below).

This change would only impact critical infrastructure assets which are captured by existing asset class definitions contained in the SOCI Act.

Material risk definition

This amendment extends 'material risks' to include risks to data storage systems which hold 'business critical data' and the systems which access that data. This amendment would:

- Not change existing requirements for critical infrastructure entities to consider cyber and information hazards or other hazard domains.
- Ensure protection of data storage systems holding 'business critical data' is considered as part of all-hazard risk mitigation, which may include consideration of physical infrastructure security.

The RMP obligation would remain a principles-based obligation. This means industry can choose their means of compliance with the RMP obligation. Industry remains required to consider other federal, state and territory regulations and ensure attestations or documents used to comply with the obligation can be produced on request. This amendment will extend to any future sector-specific RMPs beyond the current CIRMP, to preserve the efficacy and intended scope of the SOCI Act.

The proposed amendments to the above definitions will require captured critical infrastructure entities to:

- consider how threat actors could exploit vulnerabilities in systems holding business critical data;
- implement controls to mitigate or eliminate risk, prior to risks being realised;
- proactively identify and control against risks to their data storage assets as part of their CIRMP obligation;
- provide operational and ownership information regarding these systems to the CISC;
- report when a cyber incident impacts these systems under their MCIR obligation; and
- comply with directions under the SOCI Act when an incident impacting business critical data systems is having a relevant impact on their asset (for example, under Part 3A).

3.2.2 Measure 2: Improving our national response to the consequences of significant incidents – Consequent management powers

Measure 2 involves the introduction of a legislated, all-hazards power of last resort. This power would only be used where authorised by the Minister if there is no other available 'fast and effective' power.

The practical operation of the all-hazards power of last resort is outlined in the hypothetical scenario below.

Table 18 *Hypothetical scenario - operation of Measure 2*

Research data stolen from a university (Hypothetical scenario)
Scenario: As part of ongoing efforts to utilise Australian expertise for socioeconomic coercion, confidential research data could be stolen by compromising university research databases. Once stolen, this data could be used by state-based attackers to undermine other critical infrastructure systems. Malicious actors could use the stolen data to plan widespread attacks on critical services and cause disruption to functions of other critical infrastructure assets. While the university could investigate the incident and upgrade their cyber defences, the Government is uniquely placed to address the consequences for other critical infrastructure entities whose security could be impacted by the stolen data. The university may be unable to act as it does not have access to national communication channels or the asset register.
Current Outcome: In this scenario, current government assistance powers would only allow the Government to issue directions in relation to the technical cyber incident. A new consequence management power would be needed to issue directions to certain other critical infrastructure entities whose systems and critical functions have or will be disrupted due to the data breach. These directions could include directing those specific entities to upgrade information technology (IT) and operational technology (OT) security to address system vulnerabilities. If compliance with these directions would risk breaching existing contracts with IT and OT service providers, critical infrastructure entities would be able to rely on the SOCI Act's immunity provisions to avoid civil liability for such breaches.
Operation of Measure 2: If Measure 2 is implemented, the Minister would first consider whether an effective response to this scenario may be achieved using other relevant powers. If no other power is identified, issuing a direction under the all-hazards power of last resort would allow the Minister to quickly respond by: • leveraging national communication channels and asset registers to understand the potential broad impacts of the incident (including potential impacts or risks to specific entities); • directing entities to upgrade their IT and OT systems to address any system vulnerabilities, based on current threat information; and • disclosing information to other government entities or third parties affected by the breach, where necessary to inform of impacts or prevent further disruption. The Minister would be required to report use of the power under s 60 of the SOCI Act.

The scope of the power is intended to allow the Minister to authorise the following types of directions:

- Direction to a critical infrastructure entity to do or refrain from doing a certain thing to prevent or mitigate the consequences of an incident, such as a direction to address issues onsite or suspend operation.
- Authorise the disclosure of protected information as defined in the SOCI Act to allow for the sharing of information between government entities (including states and territories), between government and industry, or between the affected entity and a third party.
- Gather information for the purpose of consequence management if this does not interfere with or impede any other law enforcement action or regulatory action.

If implemented, the power would operate alongside existing government assistance powers contained in Part 3A of the SOCI Act and include the following safeguards and oversight mechanisms:

- There will be no change to the duration of a ministerial authorisation (as set out in s 35AG of the SOCI Act).
- A direction can only be given to a critical infrastructure entity.

- A direction can only be given where it is to address a consequence of an event that has occurred, is occurring or is imminent, and has had, is having or is likely to have, a relevant impact on critical infrastructure. This includes an assessment of the following:
  - There must be a demonstrable link to an incident impacting a critical infrastructure asset.
  - The incident must have a 'relevant impact', whether direct or indirect, on the availability, integrity, reliability, or confidentiality of critical infrastructure.
  - 'Imminent' relates to other critical infrastructure entities (or the affected entity) that may be compromised, or further compromised, by the inciting incident.
- A direction must not interfere with or impede a law enforcement action or regulatory action.
- The purpose of the direction is limited to preventing or mitigating serious or long-term harm to Australians or critical infrastructure or address consequences that prejudice the socioeconomic stability, national security, or the defence of Australia.
- The direction is informed by advice based on consultation with Commonwealth, state and territory agencies and regulators. The Minister must be satisfied that no existing regulatory system of the Commonwealth, a state or a territory could be used to provide a practical and effective response to the incident.
- If the power is being considered to direct the sharing of personal information, the Minister responsible for the Privacy Act (currently the Attorney General) must authorise its use, and subsequent use or disclosure of such information would be subject to the Privacy Act.
- Prior to exercising the power, the Minister must consult with the affected entity.
- The Minister must be satisfied that the responsible entity is unwilling or unable to address the consequences that prejudice the socioeconomic stability, national security, or defence of Australia, including where a legal barrier is preventing action.
- In determining whether to exercise the power, the Minister must consider the public interest – for example, whether issuing the direction is in the interest of public health and safety and is proportionate to the risk of inaction.
- Immunities would be provided in the SOCI Act to ensure that entities would not be subject to civil liability when acting lawfully in response to a compulsory legal direction.
- The periodic report under section 60 of the SOCI Act must include the number of directions issued under this power.

3.2.3 Measure 3: Enforcing Critical infrastructure risk management obligations – review and remedy powers

Measure 3 involves the introduction of a formal, written directions power to address seriously deficient elements of an RMP. This measure is related to compliance and enforcement of existing SOCI Act obligations and therefore, would not create a new regulatory burden for industry.

Under current legislative arrangements, there is no obligation for entities to provide the Department with a copy of their RMP. The Department may request a copy of the RMP, in line with the conditions specified in s 37 of the SOCI Act.

The CISC is currently undertaking trial audits of critical infrastructure entity compliance with SOCI Act obligations. Early findings are that a significant proportion of entities are not fully compliant with the existing CIRMP obligation. In addition, a significant proportion of entities are also not compliant with the requirement (which came into effect from 18 August 2024) to have a CIRMP in place that meets the relevant cyber security framework.

The SOCI National Compliance Plan 2024-25 outlines how the CISC assesses industry participants' compliance with their obligations under the SOCI Act and its associated regulations, including the CIRMP obligation. The Plan also outlines the approach to identifying entities for audit (this methodology, for security reasons, cannot be made publicly available). Under the plan, the CISC will commence compliance audit and enforcement activities for the first time in 2024-25. This change in compliance approach was flagged in the SOCI Compliance Regulatory Posture Change statement

published on the CISC website in March 2024.[25] A related enforcement framework has been developed to action non-compliance identified through audit and other compliance activities.

Subject to the passage of legislation, the new powers under the SOCI Act would then be used to mandate changes to CIRMPs that have been assessed as being seriously deficient through the audit process or following an incident. The direction to address a seriously deficient RMP may be issued where, the Department has requested the entities RMP from the entity and:

- the Secretary or relevant Commonwealth regulator has formed a view that an entity's RMP is seriously deficient, following consideration of the facts and the entity's obligations under the SOCI Act and delegated legislation. The direction would follow action from the Department to engage with entities and amend their risk practices, or in the aftermath of an incident, where the Department determines that risk assessments and mitigations are not equivalent to an entity's risk environment; and
- the deficiency carries a material risk to the socioeconomic stability, defence, or national security of Australia.

The direction may also be issued where:

- there is a severe and credible threat to national security; and
- the Secretary or relevant Commonwealth regulator is satisfied that the direction is likely to compel an effective response to address that risk.

This directions power would be accompanied by oversight mechanisms. These include the following:

- Before issuing a direction, the Secretary or relevant regulator must give a written notice that states the intention to issue a direction, reasons for the direction and invite the entity to respond.
- When deciding whether to issue the direction, the Secretary or relevant regulator must consider matters including the entity's response, any action taken, or proposed to be taken, by the entity to prevent or remedy the non-compliance, as well as the extent and degree of non-compliance.

Depending on the deficiency, the entity may exercise some discretion in how to comply with the direction. No mechanism currently exists in the civil penalty regime to effectively address wilful non-compliance with RMP requirements. In accordance with the Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers, Measure 3 includes a penalty for non-compliance in line with the existing penalty in the SOCI Act for failure to comply with a direction given under subsection 32(2) – a penalty of 250 penalty units.

3.3 Option 3: Enhanced collaboration with industry

Option 3 involves enhancing Government's collaboration with industry, through the TISN.

Under Option 3, there would be no amendment to the SOCI Act or any other legislative framework. Option 3 will include:

- Distribution of guidance on how entities may capture 'business critical data', including:
  - Suggesting that asset classes consider data storage systems which hold 'business critical data' as part of a holistic approach to their broader critical infrastructure asset, where vulnerabilities in these systems could have a 'relevant impact' on critical infrastructure.
  - Encouraging entities to ensure protection of data storage systems holding 'business critical data' are part of all-hazard risk mitigation.
- Increasing Government and industry collaboration to enhance information sharing**.** This collaboration would include:

[25] The Statement can be accessed here.

- Ongoing use of the TISN, through its various engagement mechanisms (such as online webinars, site visits, web forms and in-person workshops), allowing industry to engage directly with the Australian Government agency with portfolio responsibility for the relevant sector.

- Engagement activities focused on incident response strategies, including increasing understanding of consequential impacts of disruption, and encouraging owners and operators to share information on recovery and resilience. Compliance with response strategies would be voluntary.

The TISN's online engagement platform, which facilitates discussions across sector groups, can provide a forum for considering impacts on a cross-sector basis, given the increasingly interconnected and independent nature of Australia's critical infrastructure.

4. What is the likely net benefit of each option?

This IA identifies the anticipated costs and benefits arising from the proposed policy options. A comprehensive scan has been conducted of available literature and evidence on the impacts of the proposed regulatory changes to the SOCI Act. This scan has considered the potential benefits and regulatory costs of each policy option.

Consultation with industry on the potential reform measures provided valuable preliminary insights on the anticipated regulatory costs and benefits. A draft version of this IA (in Early Assessment format) offered an additional opportunity for industry feedback, including on the categories of costs and benefits identified and advice on the rough order of magnitude impacts of the proposed options.

This IA closely analyses written submissions from industry to:
1. Validate the expected overall impacts; and
2. Better understand and quantify (where possible) the regulatory costs and benefits arising from each option.

This IA considers the quantitative costs and benefits associated with Option 2, using a breakeven analysis. The anticipated costs and benefits of the option have significant uncertainty about size, frequency, type, sector effects and flow-on impacts beyond the entity initially impacted. Analysis of the option's total cost and benefit would be based on numerous uncertain assumptions. Consequently, this IA has instead used break-even analysis to understand the number of avoided incidents required to at least equal the estimated cost of the option. The break-even analysis also considers costs and benefits with a range of impacts to address the uncertainty about the nature and extent of incidents. Qualitative costs and benefits have been included to supplement this analysis.

For Option 1 (maintain the status quo) and Option 3 (enhanced collaboration with industry), qualitative costs and benefits have been identified and analysed. The nature of the costs and benefits for Option 3 are particularly difficult to quantify. Both costs and benefits will depend on the degree to which Responsible Entities decide to enhance their practices (as a result of engagement through TISN), and the extent to which future incidents involve Responsible Entities that have voluntarily enhanced their practices. Given the very high degree of uncertainty about these factors, assessment of Option 3 has been based on qualitative analysis.

4.1 Approach to determining costs and benefits

Costs have been identified by estimating the marginal impact on industry arising from the proposed changes. Analysis includes a mixture of cost quantification (where possible) and evaluation of actual or hypothetical case studies (where the cost impact is uncertain or highly variable in magnitude and frequency). The specific marginal costs associated with each option is set out in the sections that follow, informed by industry feedback on the type and scale of the costs expected.

The marginal impact of the proposed options will be borne by entities responsible for critical infrastructure assets who meet the relevant thresholds. Community organisations and individuals are not likely to be directly affected, noting there may be indirect costs passed onto consumers.

The benefits of each proposed measure have been identified through examination of potential disruptions arising from an all-hazards threat. The avoidance of these potential events is the principal benefit expected from the potential reform proposals. Disruption to supply, compromise of operation, or other impacts can have a significant cost to the economy. The aim of the proposed reform options is to reduce the frequency and impact of any disruption to availability, integrity, reliability, or confidentiality of critical infrastructure.

This IA uses examples of all-hazards events to demonstrate the potential direct and indirect (economy-wide) benefits which may arise from the avoidance of an incident. This approach provides sufficient reliable information to substantiate estimated incident costs. The examples demonstrate the potential disruptions to the operation of critical infrastructure assets and consider incidents with varying severities. This is because it may be the case that a series of smaller, less significant

disruptions occur over the course of a year accumulate to deliver a resulting disruption equivalent to a severe scenario (e.g. the Optus outage).

The nature of the reforms contemplated under option 2 and 3 mean that benefits are most likely to accrue on a whole-of-economy basis, rather than only to individuals or individual entities. All-hazard events are varied in their type, frequency, size and cost but commonly have an impact beyond the entity initially affected. As such, costs and benefits throughout this section focus on quantifying (where possible) the whole-of-economy impacts of incidents which may be affected by critical infrastructure assets in Australia (rather than identifying the discrete and possibly intangible costs and benefits for stakeholder groups outside critical infrastructure industry participants).

4.2 Likely net benefit assessment: Option 1 – Maintain status quo

This section outlines the qualitative costs and benefits associated with Option 1, followed by assessment of the likely net benefit derived from Option 1.

4.2.1 Costs of Option 1- Maintain status quo

Option 1 provides a baseline for costs and benefits if the status quo is maintained and can be used as a comparator with Options 2 and 3. The most significant cost associated with Option 1 is the ongoing exposure of threats to critical infrastructure which may arise where action is not taken to increase the effectiveness of the SOCI Act through the proposed reforms.

Option 1 presents risks for individuals and businesses, as gaps in the current regulatory environment may leave them more vulnerable to the impacts of an all-hazards event. For example, the recent Optus outage caused significant disruption to Australians, including an inability for 10 million Australians to access telephone and broadband services, and preventing 228 people from connecting to emergency services.[26] Similarly, the Medibank cyber incident resulted in 9.7 million Australians having their personal records stolen, including names, dates of birth, Medicare numbers, and sensitive medical information.[27] Where the status quo is maintained, industry and the Australian economy as a whole may be more likely to incur costs such as these, depending on the severity, frequency of and responses to the disruption.

Beyond potential costs to industry, other stakeholders may incur the following costs under Option 1:

- **Individuals**:
  - Gaps in the current regulatory environment may leave individuals more vulnerable to the impacts of an all-hazards event including, for example, data breaches or inhibited access to essential services.
- **Government:**
  - The realisation of an all-hazards event which can be linked to gaps in the existing regulatory framework present a significant reputational risk to the Australian Government. This danger arises from increased risks to individuals, community, and the environment.
  - From an operational perspective, the status quo limits Government's ability to intervene at appropriate points to support recovery and facilitate industry-led responses in the aftermath of an incident.

[26] https://parlinfo.aph.gov.au/parlInfo/download/committees/commsen/27530/toc_pdf/Environment%20and%20Communications%20References%20Committee_2023_11_17_Official.pdf;fileType=application%2Fpdf#search=%22committees/commsen/27530/0000%22 PG. 12

[27] https://www.foreignminister.gov.au/minister/penny-wong/media-release/cyber-sanctions-response-medibank-private-cyber-attack; https://www.medibank.com.au/livebetter/newsroom/post/medibank-cybercrime-update%207%20November

4.2.2 Benefits of Option 1- Maintain status quo

Under Option 1, individuals, industry, and Government may benefit from ongoing operation in a familiar, consistent regulatory environment, with no additional regulatory costs. Industry will also be afforded the flexibility to address all-hazard threats in a manner they see fit.

4.2.3 Likely net benefit of Option 1 - Maintain status quo

Arguments put forward throughout this IA demonstrate that Option 1 is not capable of addressing the gaps which have been identified in the SOCI Act, as this option involves no change to the Act or broader regulatory environment. While, under the status quo, industry will face no increase in regulatory costs, stakeholders will suffer the forgone benefit of consistent and clear regulation, as well as agile, industry-led responses, in the aftermath of an incident. Without the benefit of addressing these gaps, critical infrastructure is left more vulnerable to a growing threat of incidents. Industry may face the increased likelihood and consequences of all-hazard incidents.

4.3 Likely net benefit: Option 2 – Legislative Reforms

The following section details the costs and benefits associated with Option 2 followed by assessment of the overall likely net benefit presented by this option. The nature of the measures captured under Option 2 means this analysis focuses on considering the potential impacts to industry (noting any potential impacts on individuals and Government where relevant).

4.3.1 Costs of Option 2 – Legislative Reforms

This section identifies indicative costs associated with each of the three measures contemplated under Option 2.

Determining costs of Measure 1 - Amend definitions to ensure capture of 'business critical data'

Measure 1 involves amendment of definitions to ensure capture of 'business critical data'. Industry were invited to provide cost estimates on the following basis:

- Exclusive of any staff effort or costs already incurred or planned to be incurred for existing risk management activities.
- Provision of rough order of magnitude (ROM) estimates on the marginal impact on staff effort, capital and operating costs attached to Measure 1.
- ROM estimates reflect the inherent uncertainty of the cost impacts on responsible entities prior to implementation of Measure 1.
- Where uncertainty about the cost impact prevents a point estimate being provided, estimate the range of impact arising from Measure 1. The low-end range should reflect the expected cost impact. The high-end range should reflect an estimate of the 'highest feasible' cost impact.

Costs of Measure 1 - Amend definitions to ensure capture of 'business critical data'

It is expected the requirement to capture 'business critical data' in risk management activities will not have a material impact on costs incurred by industry. During consultation on the Consultation Paper and a draft version of this IA, numerous entities reported that they already protect systems and networks that hold 'business critical data' through existing SOCI Act risk management program requirements. Outside of the SOCI Act, entities may also be required to protect 'business critical data' as a result of regulation under a regime other than the SOCI Act - for example, data protected under the *Privacy Act 1998*. Therefore, the new proposed requirement under the SOCI Act would, for many entities, not result in an additional cost burden because effort (and cost) incurred to protect 'business critical data' is already occurring.

Where this is not the case, compliance with the proposal may require some additional effort but should not require the development or application of fundamentally different or new processes or standards. Risk management processes are typically applied at an enterprise-wide level and so the expanded definition is not expected to materially increase the cost of regulatory compliance beyond baseline compliance costs under the SOCI Act. Only the marginal cost uplift arising from the proposed reforms needs to be considered by this IA. Based on this analysis, the associated costs are expected to be low relative to existing costs of compliance with SOCI Act obligations.

Further, data gathered as part of the 2022 RIS included a range of costs from industry (from expected cost of compliance to the highest feasible cost of compliance with the RMP obligation). These cost ranges provided by industry allowed for identification of a quantified cost base, which has been used as the basis for quantified costs related to the current reform package. This is because:

- Costings were derived through detailed engagement with industry, across 13 of the 22 critical asset classes captured by the SOCI Act. This included industry's completion of comprehensive costing templates, which captured marginal impacts on staff effort, capital and operating costs associated with the RMP frameworks and an estimated range of impacts against each rule.
- An assessment of marginal costs arising from the proposed reforms can be undertaken to understand both (a) any cost increase for entities required to comply with the RMP framework, as well as (b) entities subject to equivalent risk management frameworks. Given these exempt entities are required to comply with a comparable regulatory framework, relevant costs for meeting baseline compliance with the SOCI Act are already incurred, creating an existing regulatory cost base which does not need to be separately considered by this IA. This IA considers the marginal uplift arising from the proposed reforms.

A summary of data collected during the 2021-22 consultation period[28] is included below.

Table 19 *Regulatory cost per entity from 2021-22 consultation period (indexed to June 2024)*

	Existing Cost ($ million)	Existing Cost ($ million)
Critical infrastructure asset	Average one-off cost per entity (submissions)[29]	Average annual ongoing cost per entity (submissions)
Critical electricity assets	9.2	4.3
Critical gas assets	12.0	2.4
Critical water assets	16.4	7.0
Critical data processing or storage assets	1.9	2.2
Critical broadcasting and domain name system assets	0.8	0.6
Critical financial market infrastructure assets (payment systems)	0.1	1.6
Critical liquid fuels assets	10.1	3.0

[28] Information about the methodology for calculating the costs from 2021-22 consultation period is provided in Appendix A of this IA. Further details on methodology and the data on which cost was based can be found in the 2022 RIS here.

[29] References in this IA to 'one-off' refer to the costs incurred by an entity to establish systems, processes and controls which will allow for compliance with the obligations.

Critical hospitals	14.8	11.5
Critical energy market operator assets	25.2	7.6
Critical freight infrastructure *and* critical freight services assets	4.4	2.6
Critical food and grocery assets	3.5	1.9
Total average cost per entity	9.0	4.1

These average costs per entity were the basis of the expected compliance with the RMP rules, outlined in the table below.

Table 20 *Summary of regulatory costs from 2021-22 consultation period (Indexed to June 2024)*

	Cost ($ million)	Cost ($ million)	Cost ($ million)	Cost ($ million)
Cost type	Industry	Community	Individuals	Total cost
One-off	$1,823.29	Nil	Nil	$1,823.93
Ongoing (per year)	$1,226.16	Nil	Nil	$1,226.16

The above expected costs were included in the draft IA distributed to industry for consultation. Industry was asked to validate, or provide commentary on the accuracy of these costs (noting industry were provided with an opportunity to validate these costs as part of the 2021-2022 consultation period).

Feedback from industry offered the following insights:

- Industry did not disagree with the cost estimates outlined in the tables above and one entity provided detailed costs which were broadly in line with the costs in Table 19.
- In most cases, industry did not provide new or different costs in relation to Measure 1.
- Where industry did provide new or different costs, these costs are comparatively immaterial relative to cost estimates for compliance with existing applicable SOCI Act obligations.

In response to the Consultation Paper, stakeholders were broadly supportive of expanding critical asset definitions to include secondary systems, such as those that hold large volumes of data, where any potential changes are balanced against the risk of regulatory duplication. Some stakeholders noted that additional detail on the nature of the policy proposal was required to allow for comment.

Overall, low numbers of submissions mean:

- Specific details on the nature of these submissions cannot be included in this IA, to prevent the identification of specific entities.
- The Department has inferred, given the extent of consultation conducted on this measure, tacit agreement from industry that additional regulation is required to ensure the protection of secondary systems.

The below table outlines the indicative costs for each sector for Measure 1, where provided through consultation feedback. Section 5 of this IA provides additional details on responses received through consultation, including how this feedback informed policy development.

Table 21 *Indicative regulatory costs for Measure 1, Amend definitions to ensure capture of 'business critical data', in each sector*

Sector	Response
Defence Industry	Respondents noted concerns about how the suggested changes will interact with the regulatory framework that currently exists within Defence Industry.
Energy	Some respondents noted an indicative cost to implement the changes of approximately $0.2m.
Financial Services	Respondents noted an indicative cost estimate of $0.1m for one-off costs.
Transport	Some respondents from this sector noted indicative cost estimates to implement the proposed changes of approximately $1.5m across measures 1, 2 and 3.
Communications Healthcare and Medical Food and Grocery Space technology Data Storage and Processing Higher Education and Research Water and Sewage	Respondents from these sectors were not able to provide indicative costs to implement this measure at this time.

For additional information on the 2021-22 cost data, refer to Appendix A.

Despite some comments from industry on a need for additional guidance and time to consider cost implications, feedback from industry did not indicate a major cost for one-off or ongoing costs to facilitate compliance with the additional clarification to protect 'business critical data'. After analysing costs provided by industry on the draft IA, the overall cost of compliance (including Measure 1) remain within the range of costs provided by industry during the 2021-22 consultation period.

Determining costs of Measure 2 - Improving our national response to the consequences of significant incidents – Consequent management powers

The expected costs of Measure 2 are variable and difficult to quantify. For the purposes of costing, it is assumed that the consequence management power will be used, on average, once every three years (frequency of 3.33 across the 10 year costing timeframe), but given the uncertainty about frequency of use, analysis also assumed the power could be used as frequently as once every year. This range in assumed frequency is in line with the use of the SOCI Act's Government Assistance measures. Since 2020, the Government has not exercised its existing power under the SOCI Act to date suggesting an expected frequency of once every three years provides a conservative estimate of cost and benefit.

Costs for Measure 2 depend on the size of entity, the duration of an incident and its consequences, the maturity of an entity's existing approaches to all-hazards risk management, and the difficulty or otherwise of complying with a direction.

Given the challenges associated with quantification in these circumstances, this IA uses hypothetical scenarios to determine categories of costs which may arise where an entity is issued with a direction. These scenarios were introduced earlier in this IA (refer to Section 1.2). Consultation on a draft version of this IA provided an opportunity for industry to validate these categories of costs and provide supporting data.

Costs of Measure 2 - Improving our national response to the consequences of significant incidents – Consequent management powers

The hypothetical scenarios below were provided to industry to help them understand and identify the categories of costs an entity may incur where they are issued a direction.

Table 22 *Hypothetical Scenario – Stolen research data*

Stolen research data (Hypothetical scenario)
Scenario: As part of ongoing efforts to utilise Australian expertise for socioeconomic coercion, confidential research data concerning vulnerabilities found across the critical infrastructure ecosystem is compromised. Once stolen, this data could be used by state-based attackers to undermine other critical infrastructure systems. Exploitation of this vulnerability is imminent and entities are at significant risk if these vulnerabilities are not addressed. Cyber incident reporting in combination with other information indicates to Government that a widespread attack will occur within the next 24 hours, across all vulnerable assets.
Operation of Measure 2: The Minister would first consider whether an effective response to this scenario may be achieved using other relevant powers. If no other power is identified, issuing a direction under the all-hazards power of last resort would allow the Minister to quickly respond by: • leveraging national communication channels and asset registers to understand the potential broad impacts of the incident (including potential impacts or risks to specific entities); • directing entities to upgrade their IT and OT systems to address any system vulnerabilities, based on current threat information; and • disclosing information to other government entities or third parties affected by the breach, where necessary to inform of impacts or prevent further disruption. The Minister would be required to report use of the power under s 60 of the SOCI Act.
Anticipated costs as a result of the consequence management power: Costs for other critical infrastructure entities associated with ongoing uplift in cyber defences and risk management processes including staff effort, capital expenditure and operating costs; Ransom demands on other critical infrastructure entities; and Loss of national research and development capability through a reduction in links between researchers and industry. Expected costs may include: 1 x Government relations - $85.17* an hour for 18 hours 1 x Senior lawyer - $3500 per day[30] 1 x middle manager - $85.17* an hour for 12 hours 4 x in house specialists – average wage - $85.17* – for 12 hours Loss of productivity for the responsible entity or entities involved in the incident, while the incident is being responded to - $500,000 Capital expenditure - $20,000 ***Costs reflect OIA guidance on work-related labour costs, available here.**

In relation to the costs outlined above, the transport sector commented that an inability to fulfil contractual requirements may result in loss of productivity cost which exceeds the figure included above. This comment confirms the highly uncertain nature of the cost impact of a Government issued direction. In this context, quantification of all possible cost impacts is difficult because (1) the

[30] Based on the Commonwealth Attorney General's Engagement of Counsel rates: https://www.ag.gov.au/legal-system/office-legal-services-coordination/engagement-counsel

consequence management power would only be used once every three years, and (2) an entity's inability to fulfil existing contractual obligations would not occur in every instance.

Table 23 *Hypothetical Scenario – Disruptions caused from non-cyber hazards*

Disruptions caused from non-cyber hazards (Hypothetical scenario)
Scenario: A series of heavy rains causes flooding which affects a facility housing a critical asset. This creates a poisonous effect in the surrounding area, putting local residents and other critical infrastructure at risk of disruption.
Operation of Measure 2: Government issues a 'do not disturb' / quarantine order for the contaminated area. If the entity is unable or unwilling to cooperate, Government directs the entity to allow emergency access to sensitive land at the facility for decontamination efforts. Using the consequence management power, the Government coordinates alternate supply of critical goods and services to preserve the services and functioning of other critical assets adversely affected by the disruption.
Anticipated costs as a result of the consequence management power: Loss of productivity/profit for affected critical infrastructure assets if they are asked to prioritise the operation of critical infrastructure ahead of existing orders/contracts. Loss of productivity/profit for entities which do not receive prioritised critical services with the severity and length of disruption impacting the extent to which prioritisation orders also affect employment in and services provided by those entities. Expected costs may include: 1 x Government relations - $85.17* an hour for 40 hours 1 x Senior lawyer - $3500 per day[31] 1 x middle manager - $85.17* an hour for 40 hours 4 x in house specialists – average wage - $85.17* an hour – for 40 hours 4 x in house specialists – overtime - $156* an hour for 20 hours Loss of productivity for the responsible entity or entities involved in the incident, while the incident is being responded to - $1,000,000 ***Costs reflect OIA guidance on work-related labour costs, available here.**

The proposed consequence management power extends existing powers in Part 3A of the SOCI Act. The potential impact of existing Part 3A powers was quantified in the 2020 RIS related to Critical Infrastructure Systems of National Significance reforms. The examples used in the 2020 RIS have been summarised below, alongside industry feedback (provided in response to the draft IA) on potential costs:

Example 1: Direction requiring a business to limit any offshore access to its industrial control systems unless approved by Government.

A transport industry participant provided that in circumstances where operational technology providers are offshore, a direction to limit offshore access has the potential to put a stop to their entire operations. As such, the costs of such direction can be in excess of $300,000 a day, depending on how reliant the day-to-day activities are on that particular control system.

[31] Based on the Commonwealth Attorney General's Engagement of Counsel rates: https://www.ag.gov.au/legal-system/office-legal-services-coordination/engagement-counsel

Example 2: A direction preventing a business from outsourcing the operations of its core network to certain low-cost, low-quality providers.

Industry commented it is unlikely to engage a low-cost, low-quality service provider. The stakeholder estimated its costs associated with core network replacement may be up to $500,000.

Example 3: A direction preventing a business from sourcing core operational systems technology from certain low-cost, low-quality providers.

An aviation industry participant provided that costs incurred will depend largely on the system involved. For example, replacing an operational technology system may also require replacement of the equipment involved. For a baggage handling system, this might be more than $50 million.

For further information on these examples and underpinning assumptions, see the 2020 RIS here. Responses to the Consultation Paper highlighted industry and individuals' concerns with a rapidly evolving risk environment. For example, consultation highlighted the increasing scale and severity of cyber incidents. Stakeholders expressed concerns on the role emerging technologies (such as generative artificial intelligence) will play in cybercrime. In addition, consultation has highlighted the following insights:

- Industry are aware that a breach of non-critical systems could provide a staging point for compromise of a critical system.
- The addition of the consequence management power in the SOCI Act will complement the Information Commissioner's existing powers, supporting a more immediate response to a cyber incident.
- The consequence management power would enable an impacted critical infrastructure entity to focus on restoring their operations, whilst the Government is able to assist with the economy-wide impacts.

The nature of the power contemplated under Measure 2 means it will not affect (or impose a cost on) all regulated entities – only a small number of entities in a small number of cases, where a direction is issued. Through consultation, industry have indicated in relation to the potential costs of a consequence management power, that:

- The allocation of costs will be contingent on critical infrastructure owners and operators complying with a direction issued by Government.
- Government should consider providing support for costs incurred by industry as a result of any directives Government may issue.

Beyond the potential costs to industry, there is a risk that Government intervention may lead to unintended consequences. However, the safeguards and oversight mechanisms set out in section 3.2.2 are designed to mitigate this risk and ensure any directions are informed by appropriate expertise. The proposed powers are intended for last resort. Proactive risk management remains the primary intended mechanism to eliminate hazards to critical infrastructure.

The broader public can be assured that Government can intervene where appropriate and as a last resort, to support incident recovery and limit the cascading impacts of an incident. This intervention should be supplemented by an ongoing partnership between industry and Government, which extends beyond the occurrence of the initial incident.

Following consultation with industry participants on the Draft IA, it is anticipated that the financial impacts of this measure could range from $0.5m to $50m per incident, with an expected incident frequency of one in every three years, suggesting an annual average cost impact of between $0.1m and $16.7m. A frequency of once every year would result in an annual average cost impact from $0.5m to $50m. These annual average cost estimates are used for the low and high range cost/benefit estimates in Table 31 below.

Table 24 outlines the emerging indicative costs for each sector for Measure 2, where provided through consultation feedback. Section 5 of this IA provides additional details on responses received through consultation, including how this feedback informed policy development.

Table 24 *Indicative costs of Measure 2 Improving our national response to the consequences of significant incidents – Consequent management powers, for each sector*

Sector	Response
Communications	Respondents noted that the cost estimations captured in the hypothetical examples of this measure are too low and that they are unable to cost the impact without additional criteria provided by the Department on potential directives it may give.
Defence Industry	Respondents noted concerns about how the suggested changes will interact with the regulatory framework that currently exists within Defence Industry.
Energy	Some respondents noted an indicative cost to implement the changes to be in the range of $1-20m.
Financial Services and Markets	Respondents noted concerns about the suggested changes and the potential for additional costs of compliance as it would depend largely on the system requirements resulting from the change.
Transport	Some respondents from this sector noted indicative cost estimates to implement the proposed changes of approximately $1.5m across measures 1, 2 and 3, with others noting a cost range of $1-50m for measure 2.
Data Storage and Processing Healthcare and Medical Higher Education and Research Space Water and Sewage Food and Grocery	Respondents from these sectors did not provide cost estimates.

Determining costs of Measure 3 - Enforcing Critical infrastructure risk management obligations – review and remedy powers

Measure 3 proposes a written directions power to direct an entity to remedy a seriously deficient RMP. Data collected during the 2021-22 consultation period provide the basis for quantification of impacts under Measure 3. This is because cost estimates captured during this consultation period for the 11 relevant sectors assumed full compliance with RMP obligations from all entities. As such, costs included in relation to Measure 3 represent enforcement costs (or costs related to non-compliance), rather than a new regulatory cost.

Costs are anticipated to range anywhere from low expense to the maximum cost indicated by the 2022 RIS, depending on the magnitude of deficiency of an entity's RMP. The expected costs associated with mandatory implementation of the CIRMP rules are taken from the 2021-22 consultation period and are outlined in Table 24 below. They include:

- A one-off aggregated cost of $1,823.92 million, across critical infrastructure assets nationally, to achieve compliance with the RMP obligations and CIRMP rules; and
- An ongoing aggregated cost of $1,226.16 million per year, across critical infrastructure assets nationally, to maintain compliance.

Table 25 *Summary of regulatory costs from 2021-22 consultation period (taken from the 2021-22 consultation period and indexed to June 2024)*

Cost type	Costs ($ million)			
	Industry	Community	Individuals	Total cost
One-off	$1,823.92	Nil	Nil	$1,823.92
Ongoing (per year)	$1,226.16	Nil	Nil	$1,226.16

In addition to the above average costs, the 2021-22 consultation period undertook analysis to determine the estimated regulatory burden by rule and obligation for each sector. This data is summarised in the tables below.

Table 26 *Regulatory burden estimate by rule and obligation (2021-22 consultation period)*

Percentage of 10 year estimate	Gas	Liquid Fuels	Water	Broadcasting
RMP obligations in the Act	7%	7%	3%	44%
General rules	3%	3%	0%	10%
CIRMP Rules				
Cyber and information security hazard	28%	28%	36%	10%
Personnel hazard	12%	12%	4%	15%
Supply chain hazard	18%	18%	4%	10%
Physical and natural hazard	24%	24%	53%	5%
Material risk	8%	8%	0%	6%
Total	**100%**	**100%**	**100%**	**100%**

Table 27 *Regulatory burden estimate by rule and obligation (2021-22 consultation period)*

Percentage of 10 year estimate	Critical Hospitals	Data	Electricity	Energy Market Operator
RMP obligations in the Act	7%	11%	10%	8%
General rules	4%	6%	2%	22%
CIRMP Rules				
Cyber and information security hazard	49%	14%	14%	25%
Personnel hazard	14%	11%	9%	5%
Supply chain hazard	7%	6%	25%	5%
Physical and natural hazard	11%	45%	25%	31%
Material risk	8%	7%	15%	4%
Total	**100%**	**100%**	**100%**	**100%**

Table 28 *Regulatory burden estimate by rule and obligation (2021-22 consultation period)*

Percentage of 10 year estimate	Food and Grocery	Freight	Payment Systems
RMP obligations in the Act	5%	28%	17%
General rules	5%	3%	9%
CIRMP Rules			
Cyber and information security hazard	42%	16%	18%
Personnel hazard	12%	7%	4%
Supply chain hazard	12%	22%	9%
Physical and natural hazard	13%	11%	14%
Material risk	11%	13%	29%
Total	**100%**	**100%**	**100%**

The costs described in Tables 25, 26, 27 and 28 were put to industry for validation in the draft IA. As with Measure 1, industry did not dispute the costs included in the 2022 RIS. Some parts of industry expressed the view that the nature of the proposed power would made provision of precise costs hard to estimate. However, the proposed costs were generally considered reasonable.

For sectors required to comply with the CIRMP rules there are no anticipated additional costs beyond the total range and estimated regulatory burden in the 2022 RIS where an entity is instructed to take

action to meet this baseline. Overall, costs of Measure 3 represent an enforcement cost, and likely falls within the range of costs provided by industry during the 2021-22 consultation period.

It is expected that the Department would intervene as little as once every 3 years to rectify a deficient RMP.

While the average cost for an entity to implement an RMP is $8.8m for one-off implementation costs, with $4m in on-going costs as defined in Table 18, the nature of Measure 3 means that exercise of the power would only require an entity to comply with an existing obligation, rather than introduce a new regulatory cost Therefore, there would be limited regulatory cost to an entity should the power be exercised. This impact is lesser still 'where only some aspects of an entity's RMP requires rectification.

Further, the average cost of $8.8 million is heavily influenced by one submission to the draft version of this IA which suggested that exercise of the power may cost up to $20 million. While this is possible, the Department considers it unlikely. The Department suggests that $2 million may be a more reasonable estimate, noting that the cost is of enforcement rather than regulatory compliance.

For additional information on use of 2021-2022 data, see Appendix A.

Costs of Measure 3 - Enforcing Critical infrastructure risk management obligations – review and remedy powers

The economy-wide costs expected to be incurred by industry as a result of Measure 3 are expected to be low. This is because:

- The impact of this measure is expected to be limited, as the directions power should only apply to a small number of entities who receive a direction to rectify a deficient RMP;
- Directions will only require compliance with the existing RMP obligations; and
- It is anticipated that the directions power will be used on average once every three years.

Based on OIA guidance on the RBMF, costs associated with measure 3 are considered non-compliance and enforcement costs because:

- Costs incurred by an entity under measure 3 will only arise where a business fails to comply with government requirements (existing RMP obligations) and action is necessary by the business to ensure compliance.
- Any new administrative processes, such as engagement with government on the contents of an entity's RMP, are considered enforcement actions and sit outside the scope of the RBMF.[32]

With reference to Tables 25 – 28 above, cost estimates captured during the 2021-22 consultation period for the 11 relevant sectors contemplate a range of cost impacts up to the highest 'feasible' cost. This analysis also considered the estimated regulatory burden by rule and obligation.

In the context of measure 3, these costs represent the costs an entity may incur to enhance their risk management practices to the baseline set by the RMP obligations. Therefore, the review and remedy power is unlikely to increase the sector-wide cost beyond the 'high' range cost already considered during the 2021-22 consultation period – as any direction issued under measure 3 represent enforcement and non-compliance costs which will not exceed the figures outlined in Tables 25 – 28 above.

Following consultation with industry participants on the draft IA, the below table outlines indicative costs for each sector. Section 5 of this IA provides additional details on responses received through consultation, including how this feedback informed policy development.

[32] https://oia.pmc.gov.au/sites/default/files/2024-02/regulatory-burden-measurement-framework.pdf PG 3-4.

Table 29 *Indicative economy-wide (or indirect) costs of Measure 3 - Enforcing Critical infrastructure risk management obligations – review and remedy powers, for each sector*

Sector	Response
Energy	Some respondents noted an indicative cost to implement the changes to be in the range of $1-20m. It is assumed these costs from industry represent enforcement and non-compliance costs – i.e., the cost of an entity being directed to rectify a seriously deficient RMP to the meet RMP obligations. These costs are expected to align with costs set out in Table 25 – 28 above.
Transport	Some respondents from this sector noted indicative cost of approximately $1.5m across measures 1, 2 and 3.
Communications Data Storage and Processing Defence Industry Financial Services and Markets Food and Grocery Higher Education and Research Healthcare and Medical Water and Sewage	Respondents from these sectors were not able to provide indicative costs to implement this measure at this time.
Cyber peak body	Respondents agreed with the changes, however, were unable to provide any cost estimates for the impacts at this time.

4.3.2 Benefits of Option 2 – Legislative Reform

The proposed reforms to the SOCI Act aim to reduce the frequency and impact of any disruption to availability, integrity, reliability, or confidentiality of critical infrastructure.

The benefits of Measure 1, amend definitions to ensure capture of 'business critical data' include:

- Increased protection for secondary systems operated by existing critical infrastructure entities.
- Reduced likelihood and severity of cyber incidents impacting these systems and reduced likelihood of migration from impacts on secondary systems to critical systems.
- Ability for Government to provide assistance when secondary systems are affected by a hazard and to limit and eliminate the consequences stemming from an incident.

The benefits of Measure 2, legislate an all-hazards power of last resort, include:

- Support from Government to seamlessly coordinate incident responses.
- Flexibility in responding to evolving threats and the potentially significant impact of an all-hazards event on the Australian economy and community.
- Allowing entities to perform actions to limit consequences that other legislation or contracts would preclude them from performing.

The benefits of Measure 3, introduce formal, written directions power, include:

- Retaining the principle-based approach to compliance, including some discretion for entities in how they respond or integrate a direction to address a deficient RMP.
- Proactively addressing and mitigating any risks which may arise because of a seriously deficient RMP.

Together, the proposed reforms enhance incident avoidance mechanisms and support the mitigation of impacts after an incident occurs, limiting disrupted operations and overall economic loss.

Option 2 will be supported by ongoing uplift and engagement through the TISN and other means, as Government remains committed to a collaborative approach to protecting critical infrastructure.

A summary of the direct impacts of each of the three measures captured under option 2 is provided in

Table 30 and Table 31 below. A break-even analysis of these benefits compared to the total estimated cost of the measures is found in Table 31. The break-even analysis is expressed as the number of incidents that would need to be avoided for the benefits (that is, the avoided costs) of the measures to equal the costs of implementation and compliance with the proposed measure

Table 30 *Summary of Scenarios*

	Low Scenario	Medium Scenario	Severe Scenario
Intensity of event	25% of Medium Scenario	Medibank data breach (2022)	Optus data breach (2022)

Table 31 *Summary of Benefits (Avoided Costs)*

	Low Scenario	Medium Scenario	Severe Scenario
Direct avoided costs (Benefits of Option)	$6.4m	$26.0m	$140.0m
Measure 1 - Amend definitions to ensure capture of 'business critical data'			
Approximate number of avoided incidents required for a net benefit*	1.2 incidents every year	1 incident every three years	1 incident every ten years
Measure 2 - Legislate an all-hazards power of last resort			
Approximate number of avoided incidents required for a net benefit – assuming intervention frequency of once every three years*	Low range estimate - 1 incident every 10 years High range estimate – 2.6 incidents every year	Low range estimate - – 1 incident every 50+ years High range estimate – 1 incident every 1.5 years	Low range estimate - 1 incident every 50+ years High range estimate – 1 Incident every 8.4 years
Measure 3 - Enforcing Critical infrastructure risk management obligations – review and remedy power			
Approximate number of avoided incidents required for a net benefit*	1.2 incidents every year	1 incident every three years	1 incident every ten years

*Note: As outlined above, the total direct one-off costs for industry entities complying with measures 1 and 3 across all sectors and asset classes are expected to be $9.0 million, with an on-going cost of $4.1 million per year. When averaged over a 10-year period, costs amount to approximately $5.0 million per year.

Noting industry responses suggesting expected costs to range from $0.5 million to $50 million per intervention for Measure 2 and assuming an expected intervention rate of once every three years, the total direct annualised costs for this measure is expected to be between $0.16 million and $16.67 million (reflected in the above table as the 'low' and 'high' break-even estimate). For the purposes of the above analysis, the expected intervention rate of once every three years was based on the usage of the power introduced in the amended SOCI legislation in 2021. The existing power has not been

used since its implementation and so for the purposes of this analysis an intervention frequency of once every three years appeared reasonable.

However, given the inherent uncertainty in this assumption, two additional intervention rates have been considered for the Measure 2 Moderate scenario above. The first assumed a more frequent intervention rate of once every two years. Under this assumption, the break-even incident prevention rate ranges from 1 incident every year (high range estimate) and 1 incident every 50+ years (low range). The second assumed a less frequent intervention rate of once every five years. Under this assumption, the break-even incident prevention rate ranges from 1 incident every 2.6 years (high range estimate) and 1 incident every 50+ years (low range estimate).

4.3.3 Likely net benefit of Option 2

The benefits of Option 2 will be at least (and are expected to be more than) the costs of the regulation. This is primarily because the marginal costs of the proposed changes are expected to be small, relative to existing costs associated with compliance under the SOCI Act and the potential avoided costs of future incidents. These direct cost impacts depend on the frequency of interventions taken by Government to enforce compliance with measures 2 and 3. However, it is noted that due to the expected frequency of interventions being once every three years, the number of avoided incidents required for total benefits to exceed the cost impact of Option 2 is also low (as set out in Table 31). The benefits of Option 2 will be at least the costs of the regulation.

The arguments put forward throughout this IA demonstrate an ongoing threat of all-hazards events, and that the severity and frequency of these events continues to grow. While some events of the magnitude described in this IA (for example, the Medicare and Optus incidents) have previously been considered to represent the worst-case disruption scenarios in Australia, the increasing severity and frequency of similar incidents, particularly in the context of growing cybersecurity incidents, represents a risk to the whole economy.

The increasing frequency of incidents makes the proposed reform measures more likely to exceed the anticipated costs over time. Through pursuit of Option 2, the prevention, mitigation, and remediation of incidents will be improved through:

- Ensuring **consistent** capture of secondary systems where vulnerabilities could have a relevant impact on critical infrastructure.
- Enabling a **coordinated, agile, industry-led response** to incidents with appropriate support from government where necessary.
- **Clarifying and enhancing** the security standards applicable to critical infrastructure.

The total economy-wide cost of these reforms are expected to be low, when compared with the losses individuals may experience during or following an all-hazards event. Government will also benefit from an enhanced partnership with industry, including an opportunity to promote industry-led recovery, and mitigate the risk of reputational damage arising from gaps in the existing regulatory regime.

4.4 Likely net benefit assessment: Option 3 – Enhanced collaboration with industry

The following section details the costs and benefits associated with option 3 (enhanced collaboration with industry), followed by assessment of the overall likely net benefit presented by this option.

4.4.1 Costs of Option 3 - Enhanced collaboration with industry

Responsible entities who choose to engage with the mechanisms available through TISN (including collaboration with Government and any guidance materials) will incur costs anywhere between option 1 (status quo) and option 2 (regulation), depending on the degree to which they decide to enhance their practices (as a result of engagement through TISN). However, given the expected economy-wide costs of compulsory implementation identified under Option 2 are likely low in relation to existing RMP impacts, costs incurred under Option 3 are also expected to be low.

For responsible entities who choose not to engage through TISN, the costs incurred will be the same as those costs associated with Option 1. This is because such entities would continue to operate under the status quo regulatory environment with an unchanged exposure to the risks identified in

Section 1 of this IA. Given these risks are growing, there are potential additional costs associated with the realisation of, for example, a cyber incident for a critical infrastructure asset. A future version of this IA will include indicative quantified costs arising from the realisation of such an incident.

Where the gaps identified in the SOCI Act are not addressed, industry and the Australian economy (including individuals, communities, and the environment) may incur additional costs, dependent on the severity and frequency of the disruption. As described previously in this IA, the current regulatory environment limits Government's ability to support industry in the aftermath of an incident. This limited ability to ensure risks are appropriately managed, compounds the potential additional costs for those entities who continue with the status quo, and enlivens a reputational risk for Government where future incidents can be linked to gaps in the regulatory regime (as is the case in Option 1).

4.4.2 Benefits of Option 3 - Enhanced collaboration with industry

Under Option 3, industry will experience some of the benefits associated with Option 2 depending on the extent that industry participates in available engagement mechanisms. Option 3 leverages shared knowledge, reduces regulatory burden, and supports the implementation cybersecurity measures. However, the realisation of benefits is inherently limited because Option 3 does not involve the introduction of all-hazards last resort or deficient RMP remediation directions power, which must be supported with legislation. These powers are crucial to supporting coordinated responses in the aftermath of an incident and contribute substantially to the benefits identified in Option 2. As such, only some elements of the existing gaps in the SOCI Act will be addressed under Option 3, including:

- Achievement of definitional clarification through enhanced collaboration between Government and industry, including the benefits of including business critical data in risk management activities;
- Knowledge of the mechanisms available under the current SOCI Act regime to support with post-incident responses, and information sharing on the most effective incident response tools; and
- Ongoing discussions between Government and industry on compliance with RMP obligations, including instances where an RMP may be deemed as deficient.

The voluntary approach may also offer industry some flexibility in choosing an approach to risk management which reflects the different risk appetites of responsible entities' and Government.

4.4.3 Likely net benefit of Option 3 - Enhanced collaboration with industry

The costs and benefits set out above demonstrate that responsible entities who choose not to engage with the TISN will not contribute to improving the current issues which exist in the SOCI Act. However, even if there were full engagement across industry, the net benefit is inherently limited by the fact that not all required reforms can be addressed through the TISN (given the requirement that directions powers are legislated).

In considering the costs and benefits described above, the net benefit of Option 3 is likely higher than pursuing Option 1, but likely lower than the net benefit offered by Option 2. This is because the voluntary format of Option 3, and the limitations on its ability to address all problem areas means it cannot address the growing threats and consequences of all-hazard incidents. Government will continue to dedicate resources to the TISN under option 2 to ensure world-class collaboration between industry and Government. Therefore, Option 3 likely presents less economy-wide benefits than Option 2.

5. Who did you consult and how did you incorporate their feedback?

This section provides an overview of the Department's consultation process for addressing the gaps identified in the SOCI Act and analysed throughout this IA. It includes a summary of the approach, outcomes and key themes emerging from consultation, as well as an explanation of the purpose and objectives of consultation.

5.1 Purpose and objectives of consultation

Continuous and broad-based consultation is an essential component of the Department's process for understanding industry and broader community views on critical infrastructure legislation and devising reforms. The Department's commitment to consultation also reflects the view that each sector manages risk in a unique way and that industry stakeholders are best placed to manage risks to their assets. The Department acknowledges and seeks to avoid broadly applicable, prescriptive legislative reforms, which have the potential to disrupt industry's ability to respond to risks in a nuanced manner.

5.2 Summary of consultation completed

The Department has completed multiple periods of consultation with industry on the proposed reform measures considered in this IA. This engagement has included:

Inviting industry to make a written submission in response to detailed questions contained in the Consultation Paper. The Paper describes each proposed measure, its rationale and indicates how the measure may operate in practice. The questions posed to industry in the paper include direct questions on how the proposed measures may impact on their business including activities which may need to be undertaken to comply with the proposed measures. To assist industry in this, a series of general town hall meetings as well as roundtables and bilateral discussions were also organised. This was supported through:

- Public town halls, advertised through the Department's social media channels and website
- Roundtables with targeted industry groups
- Presentations through the TISN sector groups
- Direct engagement with critical infrastructure entities
- Engagement with Federal, State and Territory Governments

Consultation with industry through the draft IA (which was at Early Assessment stage, though consultation preceded formal assessment by the OIA), to support identification and evaluation of potential regulatory impacts. This included a town hall specifically focused on the draft IA to ensure industry's understanding of its content and the process for responding.

- Direct engagement with Critical Infrastructure entities
- Town hall with existing critical infrastructure entities
- Engagement with Federal, State and Territory Governments

5.2.1 Feedback received through consultation on the Consultation Paper

The Consultation Paper was released on 19 December 2023, with written submissions due by 1 March 2024. A full list of the consultation questions contained in the Paper is set out in Appendix B. The Department welcomed submissions from all stakeholders including critical infrastructure entities, government, academia, and members of the public.

Industry views provided during this consultation period against each measure are outlined in the tables below. These tables also identify the Department's proposed response or actions arising as a result of industry feedback.

To support industry's understanding of the Consultation Paper and to assist in drafting written submissions, the Department hosted a series of general town hall meetings, sector-specific meetings, and bilateral discussions during the consultation period (1 March 2024). The Department also engaged directly with stakeholders through existing engagement mechanisms, including the TISN.

Face-to-face consultation also included a town hall specifically focused on the draft IA, to ensure industry's understanding of the content and the process for responding. This session allowed an opportunity for questions and answers related to a draft IA (which informed the development of the Early Assessment IA that was formally assessed by the OIA).

5.2.2 Evaluating impacts

For the proposals to achieve their goals, the Department is committed to ensuring that the benefits outweigh any regulatory impact. This requires understanding the full extent of regulatory impacts through a comprehensive IA assessment.

To supplement feedback already received from the Consultation Paper, the Department engaged in a targeted four-week consultation period to obtain views from industry on the financial impacts of the measures considered in this document. A draft version of this IA (including the consultation questions contained in Appendix C) formed the basis of discussions between the Department and industry on potential impacts.

Over 100 unique submissions were received on SOCI reforms as part of consultation on the Cyber Security Strategy Consultation Paper. The Department received submissions from all SOCI sectors with the exception of the space sector. Industry views provided in response to the draft IA have been considered throughout this document, particularly in relation to the cost benefit analysis contained in Question 4.

In many cases, feedback provided by industry on the draft IA was similar to the feedback received on the Consultation Paper. The table below summarises any additional views from industry which did not arise in relation to the Consultation Paper. A full summary of industry feedback on the draft IA is contained in Appendix C.

Table 32 *Industry sentiment and responses to the Consultation Paper*

Proposal	Summary of industry views	Department recommendation
Measure 1: Protecting Critical Infrastructure – Data systems and business critical data	**Supportive** • The intention of the proposed reform is positive, and necessary to guide entities implementation and administration of controls, to meet the updated requirements. • Limited financial impact for Authorised Deposit taking Institutions (ADI's) due to already assessing operational and non-operational systems and 'threats' to these systems. • The proposed measure will address risk and reduce regulatory burden, through the consolidation of the obligations into a single set of rules and regulations that organisations can follow. This will ensure that regulatory burden does not	• The Department notes that the intent of the amendment is to clarify the existing obligation for critical infrastructure entities to protect their assets holistically, which may include non-operational data storage assets. Expressly placing the obligation in the SOCI Act and subordinate legislation will ensure entities are proactively managing risks to the types of assets targeted in recent incidents. Recent cyber incidents to critical infrastructure have demonstrated the potential cost of uncertainty around the obligation to secure these types of assets. • The Department worked closely with the Attorney-General's Department, in response to industry feedback, to ensure amendments to the SOCI Act are complementary to existing and proposed obligations under the Privacy Act.

Proposal	Summary of industry views	Department recommendation
	become a key driver of costs and complexity.	

Measure 1: Protecting Critical Infrastructure – Data systems and business critical data	**Neutral**
	• Those entities that were neutral to the proposals recommended:
	  • Limiting the scope of business critical data to prevent unnecessary costs arising from too broad a definition.
	  • That the Department provide clear guidance material is provided to industry.
	  • Importance of aligning with the Privacy Act Review was highlighted.
	• Where cost was discussed, submissions varied on anticipated costs to comply with clarification.
		• The Department notes that the intent of the amendment is to clarify the existing obligation for critical infrastructure entities to protect their assets holistically, which may include non-operational data storage assets. Expressly placing the obligation in the SOCI Act and subordinate legislation will ensure entities are proactively managing risks to the types of assets targeted in recent incidents. Recent cyber incidents to critical infrastructure have demonstrated the potential cost of uncertainty around the obligation to secure these types of assets.
		• The Department worked closely with the Attorney-General's Department, in response to industry feedback, to ensure amendments to the SOCI Act are complementary to existing and proposed obligations under the Privacy Act.

Measure 2: Improving our national response to the consequences of significant incidents – Consequent management powers	**Supportive**
	• Majority support for this proposal, provided there is clear assurance that consequence management powers will be exercised only as a 'last resort' and appropriate safeguards and oversight mechanisms.
	• The directions power would provide the necessary authoritative and structured framework enabling coordinated and timely responses to cyber incidents that meet or exceed defined criteria. The directions power would enable:
	  • Standardised Response;
	  • Rapid Mobilisation;
	  • Impact Mitigation; and
	  • Legal Authority.
	• Proposed direction power would remove obstacles for cyber incident response and investigation procedure to be carried out in a timely manner. This would support
		• Most critical infrastructure entities are willing to do their best to address the consequences of incidents. However, in some cases, they may have legal or other restrictions, or lack the capacity to do so. As a last resort, Government should be able to assist.
		• The Department is committed to maintaining current Part 3A safeguards in response to industry feedback. Directions will only be given to critical infrastructure entities to address consequences of significant incidents impacting the availability, integrity, reliability, or confidentiality of critical infrastructure.
		• The consequence management powers are designed to be used as a 'last resort'. They will only be used where high thresholds are met, and no alternative legislative options are available. All existing safeguards in the Government assistance measures will apply as well as additional safeguards reflecting the breadth of the proposal.
		• A person who would be the subject of a direction under Part 3A would be entitled to seek judicial review under section 39B of the *Judiciary Act 1903* or

Proposal	Summary of industry views	Department recommendation
	post-incident procedures and allow for ongoing management of harm.	subsection 75(v) of the Constitution. However, the proposed consequence management powers are not intended to be subject to judicial review under the *Administrative Decisions (Judicial Review) Act 1977* (ADJR Act). • In response to industry feedback, the Department guarantees that states and territories will continue to have primary responsibility for incidents in their respective jurisdictions. However, should the consequences of an attack on critical infrastructure go beyond the initial incident, the Commonwealth Government have a strengthened capacity to support the response, through the SOCI Act. The proposed last resort power recognises these arrangements, by only being available when a critical infrastructure entity is unwilling or unable to address the consequences, and where all other regulatory levers are exhausted.

Measure 2: Improving our national response to the consequences of significant incidents – Consequent management powers	**Neutral**
	• A small number of submissions were opposed to the measure as:
	  ○ Current powers are sufficient for post-incident response, including s 32 powers.
	  ○ The scope of the power is too broad and disproportionate in the absence of further real-world case studies without appropriate safeguards, such as judicial review.
	• Care should be taken not to limit state/territory emergency and consequence management powers
		• Most critical infrastructure entities are willing to do their best to address the consequences of incidents. However, in some cases, they may have legal or other restrictions, or lack the capacity to do so. As a last resort, Government should be able to assist.
		• The Department is committed to maintaining current Part 3A safeguards in response to industry feedback. Directions will only be given to critical infrastructure entities to address consequences of significant incidents impacting the availability, integrity, reliability, or confidentiality of critical infrastructure.
		• The consequence management powers are designed to be used as a 'last resort'. They will only be used where high thresholds are met, and no alternative legislative options are available. All existing safeguards in the Government assistance measures will apply as well as additional safeguards reflecting the breadth of the proposal.
		• A person who would be the subject of a direction under Part 3A would be entitled to seek judicial review under section 39B of the *Judiciary Act 1903* or subsection 75(v) of the Constitution. However, the proposed consequence management powers are not intended to be subject to judicial review under

Proposal	Summary of industry views	Department recommendation
		the *Administrative Decisions (Judicial Review) Act 1977* (ADJR Act). • In response to industry feedback, the Department guarantees that states and territories will continue to have primary responsibility for incidents in their respective jurisdictions. However, should the consequences of an attack on critical infrastructure go beyond the initial incident, the Commonwealth Government have a strengthened capacity to support the response, through the SOCI Act. The proposed last resort power recognises these arrangements, by only being available when a critical infrastructure entity is unwilling or unable to address the consequences, and where all other regulatory levers are exhausted.
Measure 3: Enforcing Critical infrastructure risk management obligations – review and remedy powers	**Supportive** • Submissions are mostly supportive, however, clear boundaries on when the power may be used are a key theme. • Reforms are expected to instil a proactive, compliance-driven mindset, compelling organisations to enhance their continuous monitoring capabilities and prioritise risk management as a core operational focus.	• As the Department moves towards more of a compliance posture as the RMP obligations are implemented and mature, we need to have the levers in place to provide effective quality assurance. • The Department and the Office of Parliamentary Counsel have worked closely to ensure industry's expectations about the parameters of this power are met. For the purposes of this direction, the Department is proposing 'seriously deficient' to mean there is a material risk to Australia's socioeconomic stability, defence, or national security. • Industry feedback augmented the Department's commitment to always working collaboratively with entities before engaging formal powers. • Where the regulator issues a direction, the entity will be able to rectify the deficiency using the principles-based requirements for the risk management program. The CISC / Commonwealth regulator will work with the entity throughout this. • Guidance will continue to reflect the premise that the entity is best placed to assess and control against risk, and compliance will be undertaken in accordance with the CISC's Compliance and Enforcement Strategy: Cyber and Infrastructure Security Centre Compliance and Enforcement Strategy (cisc.gov.au)

Proposal	Summary of industry views	Department recommendation
Measure 3: Enforcing Critical infrastructure risk management obligations – review and remedy powers	**Neutral** • Feedback emphasised the importance of having clear parameters for when the powers may be used and ensuring the exercise of these powers is done in good faith. • Feedback emphasised the importance of consulting with industry and government when assessing a CIRMP for deficiencies.	• As the Department moves towards more of a compliance posture as the RMP obligations are implemented and mature, we need to have the levers in place to provide effective quality assurance. • The Department and the Office of Parliamentary Counsel have worked closely to ensure industry's expectations about the parameters of this power are met. For the purposes of this direction, the Department is proposing 'seriously deficient' to mean there is a material risk to Australia's socioeconomic stability, defence, or national security. • Industry feedback augmented the Department's commitment to always working collaboratively with entities before engaging formal powers. • Where the regulator issues a direction, the entity will be able to rectify the deficiency using the principles-based requirements for the risk management program. The CISC / Commonwealth regulator will work with the entity throughout this. • Guidance will continue to reflect the premise that the entity is best placed to assess and control against risk, and compliance will be undertaken in accordance with the CISC's Compliance and Enforcement Strategy: Cyber and Infrastructure Security Centre Compliance and Enforcement Strategy (cisc.gov.au)

Table 33 *Industry sentiment and responses to the Draft IA 'Amendments to the Security of Critical Infrastructure Act 2018 (Cth)'*

Proposal	Summary of industry views on proposed impact	Department response
Option 1 – maintain status quo		
Status Quo	**Supportive** • Minor costs associated with consultancy to assist in uptake and understanding of regulations. • Many entities are already familiar with obligations and operate under existing statutory and legislative frameworks which ensures compliance with the intent of the SOCI Act.	Industry feedback on option 1 improved the Department's understanding of the risk associated with the status quo and the requirement for government action. The Department also acknowledges that Option 1 imposes the lowest immediate regulatory cost on entities. However, the Department considers that the increasing prevalence of cyber-attacks and risk that Government will be unable to effectively coordinate response or work with entities to manage risks mean Option 1 could lead to significant and unmitigated events affecting Australian critical infrastructure.
	Neutral • Industry recognises the challenges in the hypothetical scenario about stolen research and development data. • Exposure to managing the risk and the cost of recovery associated with cyber incidents are likely to be greater if no further preventative action is taken.	
Option 2 – legislative reforms		
Legislative reforms Measure 1: Protecting Critical Infrastructure – Data systems and business critical data	**Supportive** • Enhancing regulatory oversight could lead to a more standardised approach to cybersecurity across critical infrastructure sectors and clearer expectations for entities.	In relation to measure 1: • The Department engaged in four weeks of consultation devoted to the impacts of the proposed measures, including. • During this consultation, industry engagement validated the expansion of definitions, to ensure implementation only occurred where necessary, with reference to risk. • Industry feedback to the Consultation Paper and draft IA informed the drafting approach taken, which narrowly defines the assets measure 1 captures. Ultimately, responsible entities for critical infrastructure assets hold the primary obligation to protect and mitigate threats to their assets. Comprehensive guidance material will continue to support industry's understanding of business critical data.
	Neutral • Rules should require all operators of critical infrastructure consider and implement appropriate safeguards against the material risks to their business critical data and associated hazards. • Responsibility for business critical data systems should be explicitly defined and sit with the entity that has primary operational control over the systems.	

Proposal	Summary of industry views on proposed impact	Department response
Legislative reforms Measure 2: Improving our national response to the consequences of significant incidents – Consequent management powers	**Supportive** • Exercise of powers will better coordinate a national response to a threat or incident.	In relation to measure 2: • The Department used information provided through the consultation process to produce mapping of all consequence management powers. • Industry provided information on existing frameworks to Government, which helped to inform the drafting approach taken. • In response to industry feedback, the Department has ensured the new consequence management power contains comprehensive safeguards and consultation requirements. Principles of proportionality are a key consideration for Government when considering the exercise of any direction. Overall, the application of this power will facilitate a coordinated uplift of post-incident response mechanisms across critical infrastructure landscape.
	Neutral • Concerns in relation to specific direction on how to mitigate a threat in the context of individual businesses. • Department should consider the complexity and bespoke nature of the unique operating environment of entities when considering the practical application of step-in powers. • The implications of this measure must be considered to ensure a step-in process is valuable and not disruptive.	
	Non-supportive • Places a burden or responsibility on entities who were not the subject of, or responsible for, a breach; for example, by directing a non-impacted entity to patch a system.	
Legislative reforms Measure 3: Enforcing Critical infrastructure risk management obligations – review and remedy powers	**Supportive** • Some respondents noted that indicative costs for compliance with this measure would be lower than indicated due to established risk management processes. • Intention of the power is supported however should consider a sector-driven and contextualised approach to review and remedy powers.	In relation to measure 3: • The Department engaged widely to ensure industry's support for the proposed regulatory changes and to guide responsible entities towards meeting their new obligations. • The Department acknowledges a desire from industry for guidance on the meaning of 'seriously deficient'. This guidance (on this and other matters) will be developed after the legislation's introduction.

Proposal	Summary of industry views on proposed impact	Department response
	Non-supportive • Insufficient time has passed since the establishment of the CIRMP, to understand if this power is required. • Could also impose significant compliance costs, reduce flexibility for entities to manage risks according to their specific circumstances, and potentially stifle innovation due to more prescriptive requirements.	• The Department still maintains that entities are best placed to manage risks to their assets. • In response to the feedback provided by industry, Government remains committed to exercising the direction in the most extreme cases only, after consultation with an entity has been attempted. • Government remains committed to principles-based regulation and will only direct entities when their RMP fails to produce the outcomes required by principles-based legislation.
Option 3 – Enhanced collaboration with industry		
Enhanced collaboration with industry	**Supportive** • Feedback mostly agreed that expected impacts were accurately described. • This option gives entities flexibility in determining which enhancements would provide material risk reduction and proceed to enhance practices accordingly. • For consequence management this option enables the development of a framework and supporting flow chart of predetermined actions in the event of a critical incident. • Some entities indicated that there would see minimal change to company policy, but would still produce intended benefits	• Collaboration through the TISN will continue regardless of the selected policy option, as the TISN is a strong and proven resource for effective collaboration between industry and Government. • However, similarly to Option 1, the TISN it is limited in what it can achieve, particularly in areas that require consistent application across critical infrastructure sectors. Industry feedback also underscored the risks of pursing a voluntary approach to security-related regulation.

Proposal	Summary of industry views on proposed impact	Department response
	Neutral • Australia's CI is too important, and the cyber risks are too great to have a voluntary initiative to increase cyber protections. • The TISN remains an important body, however Government must establish stronger standards and advisories for critical infrastructure, which is not able to be achieved through the TISN. • Consideration for structure to enable industry collaboration and drive targeted, pragmatic outcomes in recognising sector challenges.	• Industry feedback helped to understand the value of the TISN from industry's perspective and how it could be strengthened under any option.

6. What is the best option from those you have considered and how will it be implemented?

6.1 Best option from those considered

The preceding consultation outcomes and analysis has demonstrated that Option 2: Amend the SOCI Act is the most suitable option from those considered.

Section 3 of this IA identified the objectives of Government action. These objectives align with, and seek to address, the elements of the problem discussed in Section 1 below demonstrates that amendments to the SOCI Act (through the 3 measures under consideration) will support each of Government's objectives for intervention and comprehensively address the problems identified and discussed throughout this IA.

Table 34 *Assessment of Option 2 against objectives and problem elements*

	What is the problem?	What are Government's objectives?		Why Option 2?
1.1	There is a growing number of cyber incidents which impact non-operational data storage systems held by critical infrastructure entities and can often be a point of entry for malicious actors.	• Ensure **consistent** capture of secondary systems where vulnerabilities could have a relevant impact on critical infrastructure.	✓	Option 2 addresses the ambiguity in existing legislative arrangements in relation to the capture of non-operational data CI assets, and corresponding Government objectives, in a number of ways: • Increasing protection for secondary systems operated by existing critical infrastructure entities. • Reduced likelihood and severity of cyber-attacks on these systems. • Assistance in mitigating the consequences of these incidents on critical infrastructure.
1.2	Businesses often face difficulties responding effectively in the aftermath of significant incidents because of legal risks and government's limited ability to support with post-incident consequence management.	• Enable a **coordinated, agile, industry-led response** to incidents with appropriate support from government where necessary.	✓	Option 2's consequence management powers will allow Government to collaborate with industry and have the ability to provide further assistance in response to an incident occurring. Such collaboration will provide Government with insights into each CI asset's operating environment and be able to provide appropriate support when deemed necessary. Option 2 will allow Government the benefit from an enhanced partnership with industry, including an opportunity to promote industry-led recovery, and mitigate the risk of irrecoverable damage with limited support for post-incident response arising from gaps in the existing regulatory regime; through: • Support from Government to seamlessly coordinate incident responses.

	What is the problem?	What are Government's objectives?		Why Option 2?
				• Flexibility in responding to evolving threats and the potentially significant impact of an all-hazards event on the Australian economy and community.
1.3	When an entity is unwilling to comply with the regulator's recommendations to enhance an RMP, there is no ability for the regulator to issue a direction that the entity remedy the deficient RMP.	• **Clarify and enhance** the security standards applicable to critical infrastructure. • Enable an **agile, industry-led response** to incidents with appropriate support from government where necessary.	✓	The introduction of a directions power under Option 2, when an entity's RMP is deemed seriously deficient, will improve the security standards and resilience of critical infrastructure assets. This is because Government will have the ability to take action and direct that an entity uplift the security and resilience of their assets to meet required standards. The Government will ensure that risk management programs are being implemented appropriately and prioritised by responsible entities; including: • Retaining the principle-based approach to compliance, including some discretion for entities in how they respond or integrate a direction to address a deficient RMP. • Proactively addressing and mitigating any risks which may arise because of a deficient RMP. • Providing guidance to industry on the meaning of 'seriously deficient' following the passage of legislation.

The summary contained in table 34 above indicates that Option 2 is the best option. This is primarily because amending the SOCI Act is only option capable of addressing each problem area identified in this IA. It achieves the objectives of Government intervention and stands to deliver substantial benefits to industry and the Australian economy as a whole. Conversely, Table 35 below draws on the analysis undertaken in Section 4 above, to highlight Option 1 and 3's inability to address the identified problem areas and meet Government's objectives for intervention.

Table 35 *Assessment of Options 1 & 3 against objectives and problem elements*

	What is the problem?	What are Government's objectives?		Why not Option 1 or 3?
1.1	There is a growing number of cyber incidents which impact non-operational data storage systems held by critical infrastructure entities, which can often be a point of entry for malicious actors.	• Ensure **consistent** capture of secondary systems where vulnerabilities could have a relevant impact on critical infrastructure.	✖	**Option 1:** If the status quo is maintained, identified vulnerabilities and corresponding risks in relation to the increase in cyber incidents which have the ability to impact data storage systems, and corresponding Government objectives, cannot be met. This means: • There will be no consistent framework across the sector which accounts for secondary systems vulnerable to malicious attacks. • Responsible entities will not be compelled to identify and mitigate risks in relation to vulnerabilities in their secondary non-operational systems. • Organisations, and the economy, may incur substantial costs should disruptions affecting the operation of critical infrastructure assets occur. The costs will depend on an incident's frequency, severity and critical infrastructure assets affected. **Option 3:** Under a voluntary arrangement, identified risks of additional secondary non-operational data system held by critical infrastructure entities can only be addressed to the extent that responsible entities choose to participate in the framework. In addition, the associated Government objective to relieve this vulnerability will not be met as legislative protection will be inconsistent amongst the critical infrastructure ecosystem.

	What is the problem?	What are Government's objectives?		Why not Option 1 or 3?
1.2	Businesses often face difficulties responding effectively in the aftermath of significant incidents because of legal risks and government's limited ability to support with post-incident consequence management.	• Enable a **coordinated, agile, industry-led response** to incidents with appropriate support from government where necessary.	✖	**Option 1:** If the status quo is maintained, there will be no improvement to businesses ability to respond effectively to the aftermath of an incident, nor allow Government to adequately provide support and guidance for post-incident responses. **Option 3:** Under Option 3, the implementation of measure two in a voluntary format may facilitate a stronger relationship between some industry stakeholders and Government. This will be the result of Government providing appropriate support and guidance for entities post incident. However, this will not be achieved across the critical infrastructure ecosystem. Whilst industry seeks accompanying guidance material with the directions power that will be awarded to Government, if measure 2 is implemented on a voluntary basis, improvement to post incident industry response and Government's flexibility in responding to evolving threats with potentially significant impacts will be limited, including through existing legal obstacles. This is specifically in relation to impact mitigation and the ability for Government to direct a business to enact response plans. As such, a voluntary approach would only enhance the current imbalance and transparency of security in oversight mechanisms of critical infrastructure organisations differing State and Territory emergency management frameworks.

	What is the problem?	What are Government's objectives?		Why not Option 1 or 3?
1.3	When an entity is unwilling to comply with the regulator's recommendations to enhance an RMP, there is no ability for the regulator to issue a direction that the entity remedy the deficient RMP.	• **Clarify and enhance** the security standards applicable to critical infrastructure. • Enable an **agile, industry-led response** to incidents with appropriate support from government where necessary.	✖	**Option 1:** Status quo legislative arrangements do not provide nuanced regulations, which support entities in implementing efficient RMPs. Existing enforceable undertaking measures are too time consuming and costly (for both the Department and affected entity), leaving open the risk that vulnerabilities from a deficient RMP materialise in the course of seeking an enforceable undertaking. Further, there would be no uplift in risk management practices, or the security standards of entities and their protection and resilience of their critical infrastructure assets. Without sector-wide concerted efforts to uplift security standards and RMP's to provide defences against hazards and an asset-wide uplift in the security and resilience of critical infrastructure assets, the Australian economy as a whole may incur significant cost. **Option 3:** A voluntary framework means that the risks to critical infrastructure assets which RMPs seek protect will only be lowered to the extent that entities choose to participate in the framework. This will lead to an inconsistent uplift in responsible entities' compliance with relevant security standards. Given the interconnected nature of critical infrastructure assets improvements to RMPs and thereby security and resilience of such assets will be limited, where the framework is not implemented on a sector-wide, mandatory basis.

As demonstrated in Table 35 above, Options 1 and 3 are not capable of solving the policy problem, nor aligning with the Government objectives for intervention outlined by this IA. Without implementing Option 2 as demonstrated in Table 35 above, amendments to the SOCI Act, the identified problem areas cannot be addressed, Government's objectives for intervention cannot be met, and industry and the Australian economy as a whole will not experience, to the full extent, the avoided costs outlined above.

6.1.1 Net benefit comparison

In addition to the above analysis, direct comparison of the net benefit of each of the three policy options considered in this IA also supported identification of Option 2 as the preferred option.

***Table 36** Direct net benefit comparison*

Option	Net benefit summary
Option 1: Status quo	• Option 1 is not capable of addressing the gaps which have been identified in the SOCI Act, as this option involves no change to the Act or broader regulatory environment. • The benefit of industry facing no increase in regulatory costs is outweighed by the forgone benefit of consistent and clear regulation, and agile, industry-led responses post-incident. • Without these benefits, critical infrastructure is left vulnerable to a growing threat of incidents. Industry may face the increased likelihood and consequences of all-hazard incidents.
Option 2: Amend the SOCI Act	• Benefits of Option 2 will be at least (and likely more than) the costs of the regulation. This is primarily because the marginal costs of the proposed changes are expected to be small, relative to existing costs associated with compliance under the SOCI Act and the potential avoided costs of future incidents. • Due to the expected frequency of interventions being once every three years, the number of avoided incidents required for total benefits to exceed the cost impact of Option 2 is also low (as set out in Table 31). The benefits of Option 2 will be at least the costs of the regulation. • The increasing frequency of incidents makes the proposed reform measures more likely to exceed the anticipated costs over time. • The total economy-wide cost of these reforms are expected to be low, when compared with the losses individuals may experience during or following an all-hazards event.
Option 3: Enhanced collaboration with industry	• The net benefit of Option 3 is inherently limited by the fact that not all required reforms can be addressed through the TISN (given the requirement that directions powers are legislated). The net benefit of Option 3 is likely higher than pursuing Option 1, but likely lower than the net benefit offered by Option 2. This is because the voluntary format of Option 3, and the limitations on its ability to address all problem areas means it cannot address the growing threats and consequences of all-hazard incidents. • Government will continue to dedicate resources to the TISN under any option to ensure world-class collaboration between industry and Government.
Overall Comparison	Direct comparison of the net benefit of each option supports identification of Option 2 as the preferred option because: • It is the only option capable of addressing the problem areas identified in Section 1 of this IA; • While the overall costs are higher as compared to Options 1 and 3, the net benefit is also higher; and • The increasing frequency of incidents means benefits of Option 2 are more likely to exceed the costs overtime.

6.2 Implementation

Although it offers the best option from those considered, Option 2 is not without risks. Effective implementation of proposed amendments to the SOCI Act is essential for ensuring Option 2's benefits are realised in their entirety. This IA, including stakeholder feedback, risks and implementation considerations, will accompany the passage of the proposed legislative amendments to inform a final decision (in line with the table below).

Table 37 *Summary of policy development*

Policy development stage	Relevant IA development stage	Dates
Detailed consultation paper on the nature of the proposed reform measures for industry	Draft IA	19 December 2023 – 1 March 2024
Detailed consultation on the nature of the proposed reform measures to support an Exposure Draft of the Bill (however was unable to be released with the Exposure Draft)	Early Assessment IA	March 2024
Decision by Government to implement proposed reform measures	First Pass IA	July 2024
Final decision by Government to implement proposed reform measures	Second Pass IA	Spring 2024

The risks associated with Option 2, as well as a proposed implementation, monitoring and evaluation plan are discussed below.

6.1.1 Approach to implementation

This section outlines the Department's proposed implementation plan, including an outline of key implementation tasks, and the challenges or risks associated with implementing the proposed amendments to the SOCI Act. Evaluation considerations, including an evaluation plan, are contained in section 7 below.

Government's objectives for implementation are to introduce amendments to the SOCI Act in a manner which ensures affected industry stakeholders:

- Understand and comply with their new or expanded obligations under the amended SOCI Act;
- Continue to engage with Government to identify, understand and mitigate risks which exist in the sector, and collaborate to drive the implementation of strong security standards and expedient responses in the aftermath of an incident; and
- Receive appropriate and consistent direction, assistance, and guidance from Government, to allow for compliance with new and expanded obligations.

Implementation plan

Effective implementation requires the completion of several key steps, identified below in Figure 1. Additional detail on these activities is set out in

***Figure 1**: Overview of implementation plan*

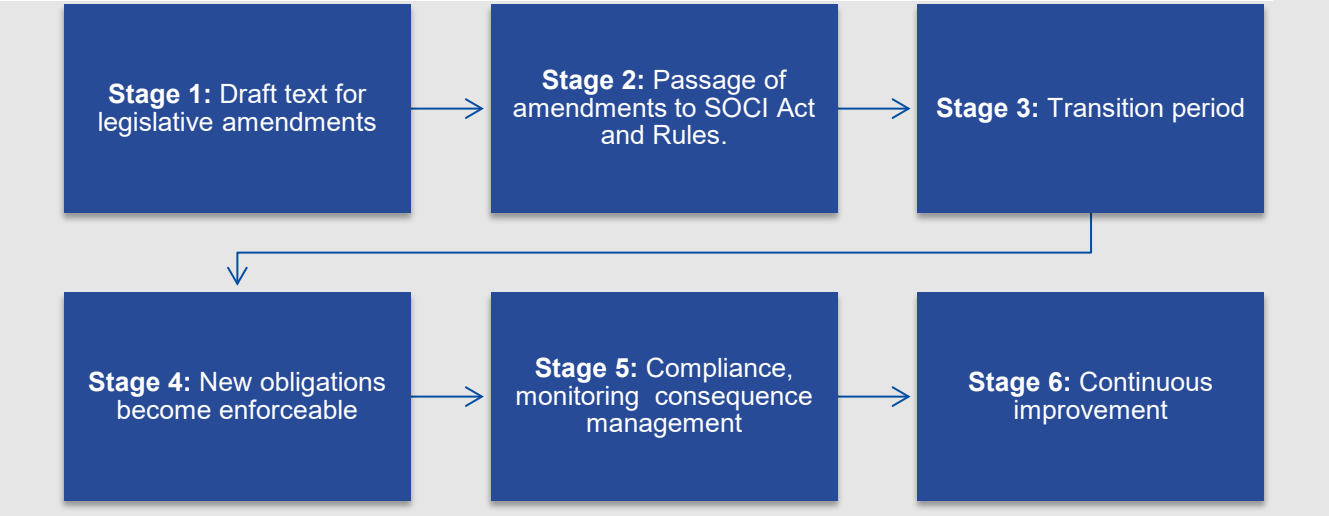


***Table 38** Detail on implementation activities*

Stage	Activities
Stage 1	Complete consultation with industry on proposed amendments, including on regulatory impacts. Prepare draft text for amendments (incorporating industry feedback) for consideration by Government.
Stage 2	Passage of amendments to the SOCI Act and subordinate legislation. Preparation and publication of guidance material for industry on compliance with obligations, which may include: ○ Case studies ○ Frequently asked questions; ○ Guidance and engagement through the TISN; and ○ Insights into best practice and Government's expectations.
Stage 3	Commencement of transition period where industry commence undertaking activities to become compliant with expanded obligations (where relevant). For example, capture of secondary systems in the definition of 'material risk'. Measure 1 will be in effect once the legislation and updated rules are in force, while measures 2 and 3 will only be used as needed and as a last resort. Education and engagement Preparation of policies and procedures for compliance activities.
Stage 4	Enforcement of expanded obligations commences.
Stage 5	Post-implementation review of amendments. May form part of the legislative independent review of the SOCI Act, required under s 60A.
Stage 6	Implementation of formal and informal regular feedback mechanisms, including through the TISN. Possible updates to guidance materials in response informal feedback from industry.

Regulatory functions

The Department has regulatory powers under the SOCI Act, through provisions contained in the *Regulatory Powers (Standard Provisions) Act 2014*. Monitoring and compliance activities will be conducted by the Department, who will continue to discharge their relevant regulatory function across

Australia's critical infrastructure sectors.[33] The Department continues to engage and coordinate with existing critical infrastructure regulators across the various sectors.

The Department will continue to report on its regulatory activities, including the implementation of expanded obligations, in its annual report to Parliament as required by section 60 of the SOCI Act.

Approach to compliance

The Department specifies five principles which provide guidance in the exercise of its regulatory powers and engagement with industry.[34]

***Table 39**: Departments regulatory principles*

Principle	Meaning
Focus on risk	• Focus attention and resources on higher risk areas to ensure the resilience and security of the sectors we regulate.
Promote voluntary compliance	• Where appropriate, adopt a consultative approach with industry stakeholders. • Solicit feedback to inform continuous improvement within the critical infrastructure sectors. • Provide education and guidance to help industry partners understand their legislative obligations.
Be accountable, fair, and transparent	• Avoid unnecessarily impacting the efficient and effective operations of responsible entities. • Make timely decisions based on legislative requirements.
Act consistently	• We deliver equitable decision-making across a variety of critical infrastructure sectors and situations.
Act proportionately	• When exercising enforcement powers, we consider the: ○ security implications of the non-compliance; ○ seriousness of the non-compliance; ○ compliance history and regulatory posture of the entity; ○ need for deterrence; ○ facts of the matter at hand; and ○ impact on Australia's reputation or Australian interests overseas.

These principles inform the way in which the Department's regulatory functions engages with industry including, wherever possible, working in partnership with regulated entities to manage and understand risk. This approach reflects the Department's vision for voluntary compliance with the SOCI Act by owners and operators and ultimately, the effective management of security risks across all critical infrastructure sectors.

Where non-compliance is observed, the range of options available include:

- education and engagement
- non-compliance and observation notices
- corrective action plans
- infringement notices
- directions
- enforceable undertakings
- enforcement orders
- suspension or revocation of authorisations

[33] This is the case for all sectors, except critical payment systems where the Reserve Bank of Australia is the regulator.
[34] https://www.cisc.gov.au/legislation-regulation-and-compliance/our-regulatory-principles-and-approach

- prosecution.

The Department selects the most appropriate approach to compliance, based on the objectives of the legislation.

In 2023-24, the Department's compliance focus has been on education and awareness. This approach has ensured that industry understands and seeks to comply with applicable obligations under the SOCI Act.

The CISC is currently undertaking a limited series of trial audits to test industry compliance with existing SOCI Act obligations. This will inform and guide the commencement of compliance audit activities in 2024-25, which will aim to balance education and awareness raising activities with compliance activities. This approach aims to effectively drive an uplift in regulated entity compliance. This approach will not impact on the transition period proposed by the Department for expanded obligations which arise from the amendments to the SOCI Act contemplated in this IA.

6.1.2 Challenges and risks to implementation

There are several challenges and risks which could impede the Department's successful implementation of amendments to the SOCI Act. These challenges and risks are identified in table 41 below, and rated in terms of their likelihood and consequence, in accordance with Table 40.

Table 40 *Likelihood and consequence ratings*

Likelihood		Consequence	
Low	The identified risk or challenge is unlikely to eventuate.	**Minimal**	If the identified risk or challenge does eventuate, it would have a limited effect on the Department's ability to implement the proposed measures.
Medium	It is reasonably possible that the identified risk or challenge will eventuate.	**Moderate**	If the identified risk or challenge does eventuate, it would have a substantial effect on the Department's ability to implement the proposed measures.
High	It is likely that the identified risk or challenge will eventuate.	**Severe**	If the identified risk or challenge does eventuate, it would have a significant effect on the Department's ability to implement the proposed measures.

Table 41 *Challenges and risks to implementation*

Challenge or risk	Likelihood	Consequence	Management
Lack of industry awareness of amendments: Some industry stakeholders may be unaware of the amendments, or the extent of their obligations under the amended SOCI Act	**Low**	**Severe**	The Department has led consultation with industry, to provide context on the proposed reforms and elicit feedback. This consultation included town hall forums, round tables, and open feedback forums. Consequently, it appears unlikely that any affected entities would be unaware of the upcoming introduction of the reform measures to the SOCI Act. Following a presentation to industry of the Draft IA; consultation period provided a further opportunity to build industry's awareness of, and receive feedback on, the proposed measures.

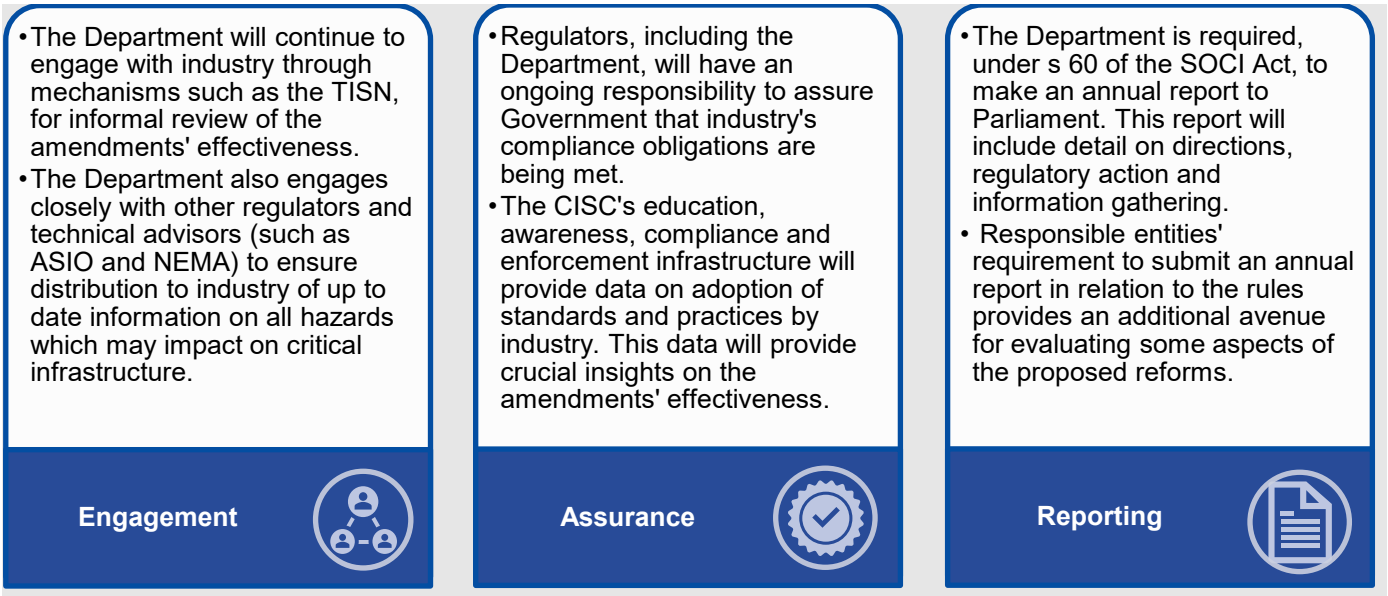
Challenge or risk	Likelihood	Consequence	Management
Government capability: Insufficient funding or understaffing could impact on the effectiveness of the proposed reforms, especially in relation to compliance activities.	**Medium**	**Severe**	The Department will be able to utilise current resourcing for Measures 1 and 3. For Measure 2, resourcing and capability development may be required to ensure officials engaging with industry are knowledgeable, highly skilled at identifying vulnerabilities in critical infrastructure assets, and are able to support the Department's regulatory role.
Implementation costs: There is a risk that the expected costs of implementation are either over or underestimated by industry and within this IA.	**Medium**	**Moderate**	Requesting that industry include a cost range when providing costing data may mitigate the risk that costs to industry could be higher than anticipated.

7. How will you evaluate your chosen option against the success metrics?

7.1 Approach to evaluation

The effectiveness of the proposed amendments to the SOCI Act will be assessed on an ongoing basis. This will include through Parliamentary processes and ad hoc feedback from industry and Government stakeholders (including through mechanisms such as the TISN).
Mechanisms for review of the amendments are outlined in Figure 2 below.

Figure 2 *Evaluation mechanisms*



7.1.1 Approach to evaluation - Measure 1 - Protecting critical infrastructure – Data storage systems and business critical data

Evaluation on the effectiveness of Measure 1 will be through:

- Analysis of relevant cyber incident data sources, including annual RMP annual attestations, RMP audits, and cyber incident reports and follow-up investigations with relevant regulators, agencies and critical infrastructure entities.[35]
- Cyber incidents affecting critical infrastructure, particularly those caused by lateral movement from data storage systems that hold business critical data. The Cyber Security Strategy's, proposed Cyber Incident Review Board (CIRB), may enable suitable oversight and understanding for analysis. Analysis from the CIRB will inform the Department's understanding of cyber incident trends and may assist to evaluate long term reductions in incidents affecting relevant critical infrastructure data storage assets.

[35] Note: For security purposes, the process for RMP sampling and audit methodology will not be made publicly available.

7.1.2 Approach to evaluation - Measure 2: Improving our national response to the consequences of significant incidents – Consequent management powers

Evaluation on the effectiveness of Measure 2 will be through:

- Analysis of end-to-end incident response. The proposed CIRB, under the Cyber Security strategy may allow sufficient oversight of the use of the power.
- The use of this power will be reportable to the Minister for presentation in Parliament as part of s 60 of the SOCI Act.

7.1.3 Approach to evaluation - Measure 3: Enforcing Critical infrastructure risk management obligations – review and remedy powers

It is anticipated that use of this power will be reportable to the Minister as part of s 60 of the SOCI Act. This will form the basis of the evaluation of effectiveness.

7.2 Indicators of success

Amendments to the SOCI Act will ensure effective identification, assessment, and mitigation of risks, enhancing industry's ability to respond to critical infrastructure disruptions.

If implemented successfully, the amendments to the SOCI Act will:

- Allow Government, industry, and the Australian public to have ongoing confidence in the resilience of our critical infrastructure providers;
- Ensure the provision of adequate support from Government to industry in the aftermath of an incident; and
- A strengthened relationship between industry and Government through heightened and more frequent engagement, knowledge, and awareness of the Department's approach to compliance, and improved visibility for both industry stakeholders and Government.

Section 60A of the SOCI Act requires the conduct of an independent review of the operation of the SOCI Act. The timing and focus of this independent review is a matter for Government. The amendments to the SOCI Act contemplated in this IA will be captured by this review process.

The above indications of success align with Government's objectives for intervention, as outlined in table 42 below.

Table 42 *Alignment between Government objectives and outcomes*

Government objectives	Indicator of success	Evidence of Success
Ensure **consistent** capture of secondary systems where vulnerabilities could have a relevant impact on critical infrastructure.	All relevant secondary systems are captured by regulation, reducing the risk of adverse impacts on critical infrastructure.	Industry reporting on approaches to risk management for secondary systems. Specifically: • A stronger understanding of the need to capture secondary systems and the indicators of malicious attacks; and • A reduction in the number of (or severity of) critical infrastructure attacks arising through secondary systems.
Enable a **coordinated, agile, industry-led response** to incidents with appropriate support from government where necessary.	Industry are equipped and informed to deal with incidents, including when to seek Government support.	Industry reporting on approaches to incident response management. Specifically: • A stronger understanding of the ways in which industry can best respond; and • A flexible and transparent approach to interactions with Government, including leveraging Government support at appropriate points.
Clarify and enhance the security standards applicable to critical infrastructure.	Industry have a clear view on applicable standards.	Industry reporting on applicable standards. Specifically: • An ability to clearly identify, implement and comply with standards applicable to their relevant asset.

Appendix A: References to the 2022 RIS

Approach to 2022 RIS

The 2022 RIS related to the introduction of a framework for risk management for a selection of asset classes. This framework, now contained in Part 2A of the SOCI Act, requires responsible entities to have and adhere to a critical infrastructure RMP.

The asset classes captured by the 2022 RIS (and required to comply with Part 2A of the Act) are:

- Critical broadcasting assets;
- Critical domain name systems'
- Critical data storage or processing assets;
- Critical electricity assets;
- Critical energy market operator assets;
- Critical gas assets;
- Designated hospitals (a subset of 'critical hospitals');
- Critical food and grocery assets;
- Critical freight infrastructure assets;
- Critical freight services assets;
- Critical liquid fuel assets;
- Critical financial market assets that are used in connection with the operation of a payment system (as per s 12D(1)(i) of the SOCI Act); and
- Critical water assets.

The cost benefit analysis contained in the 2022 RIS examined the implementation of the RMP framework, based on the requirements now contained in Part 2A of the SOCI Act and the CIRMP rules. The cost benefit analysis also considered the required uplift in risk management practices across Australia's critical infrastructure assets, and resultant improvement in the security and resilience of interconnected critical infrastructure across Australia. However, this analysis only considered (and quantified the costs attached to) the uplift for the asset classes where the CIRMP rules would be 'switched on'.

Approach to 2022 RIS cost benefit analysis

To quantify the regulatory proposal set out in the 2022 RIS, each responsible entity was asked to complete a template to estimate costs of compliance with the RMP obligations, using the following basis for estimate:

- **Rough order of magnitude estimates** to reflect the inherent uncertainty of the cost impacts on responsible entities prior to the legislation being switched on.
- **Marginal impact on staff effort and/or capital/operating costs** as a result of the proposed Risk Management Program Framework. Staff effort or costs that are already incurred or planned to be incurred were excluded from estimates.
- **Estimated range of impact against each obligation/rule**. The low-end range was the expected cost impact. The high-end range was an estimate of the 'highest feasible' cost impact.
- **Cost estimates were provided in constant ('today') dollars**. The cost estimates were not escalated or indexed.

Following receipt of inputs from industry, the methodology outlined in Table 43 below was used to determine costs and benefits.

***Table** 43 Methodology of 2022 RIS for Cost Benefit Analysis*

Step	Description

1. Calculate estimated cost of compliance for each responsible entity.	• Submissions from responsible entities were analysed to determine the estimated cost of compliance for each entity.
	• To calculate the estimated cost of compliance for each entity, the following formulas were used:
	  ○ Total labour cost = marginal staff effort x standard unit labour price
	  ○ Total cost of compliance = total labour cost + marginal capital costs + marginal operating costs

2. Extrapolate sector wide costs of compliance	• Sector wide costs were extrapolated from the estimated costs for individual responsible entities. Costs were broken down by sub-sector (where relevant) and size (large and small entities).
	• Throughout the costing process:
	  ○ An analysis of the average cost per obligation/rule (expressed as cost per entity, cost per rule per employee, cost per rule per critical site, etc) was undertaken. This analysis assisted in validation of the cost estimates provided.
	  ○ The size of estimated ranges was reviewed to determine the confidence and certainty about the impact of each obligation/rule.
	• A total estimated cost for whole of sector compliance with the full RMP was calculated.

3. Estimate benefits	• Benefits were determined by identifying and quantifying the whole-of-economy impact of a range of scenarios, based on actual all-hazards incidents that have occurred in Australia. Benefits were then calculated on the basis of the avoided costs of these scenarios with the reasonableness of these assumptions based on actual historical impacts.
	• This approach was taken for the following reasons:
	  ○ Benefits will be accrued on a whole-of-economy level, rather than to specific organisations or individuals.
	  ○ The total benefits of the RMP were unable to be estimated, as they largely consist of the costs of avoiding or mitigating future all-hazard incidents about which there is no data on the frequency and size. Consequently, any estimate of total benefits would be highly uncertain and assumptions based.
	• In addition to quantified benefits, qualitative benefits will also be documented and evaluated.

4. Validate net benefits and validate with industry.	• A breakeven analysis was conducted to determine the number of scenarios required to occur to equal the costs of compliance with the RMP. • The full text of RIS Question 4 was shared and validated with industry, and feedback was incorporated.

Computable General Equilibrium (CGE) modelling approach

To analyse the direct and indirect economic contributions of a disruption to critical infrastructure on the Australian economy, a CGE approach modelled the economy as a system of interrelated economic agents operating in competitive markets. Economic theory is used to specify the behaviour and market interactions of economic agents, including consumers, investors, producers, and governments operating in domestic and foreign goods, capital, and labour markets.

Defining features of the theoretical structure of the model are:

- Optimising behaviour by households and businesses in the context of competitive markets with explicit resource and budget constraints;
- The price mechanism operates to clear markets for goods and factors such as labour and capital (i.e. prices adjust so that supply equals demand); and
- At the margin, costs are equal to revenues in all economic activities.

The modelling framework is suited to analysing the economic impact of events impacting interconnected critical infrastructure assets as it explicitly captures supply-chain linkages as well as other flow-on effects and feedback responses by all economic agents. The strength of CGE models is that they capture the upstream and downstream linkages between the activities induced by the event and the rest of the economy in a framework that combines detailed historical data with fundamental economic theory.

The CGE modelling provided estimates on the Australian economy's sensitivity to a shock. The method consisted of defining a hypothetical baseline scenario through researching real-world incidents and understanding the various costs and price impacts associated with the event.

2022 RIS as a costing baseline

In assessing Measures 1 and 3 under Option 2, this IA uses the quantified cost base calculated through the 2021-22 consultation period with industry, as the basis for quantified costs related to the current reform package. This is because:

- Costings were derived through detailed engagement with industry, across 13 of the 22 critical asset classes captured by the SOCI Act. This included industry's completion of comprehensive costing templates, which captured marginal impacts on staff effort, capital and operating costs associated with the RMP frameworks and an estimated range of impacts against each rule.
- An assessment of marginal costs arising from the proposed reforms can be undertaken to understand both (a) any cost increase for entities required to comply with the RMP framework, as well as (b) entities subject to equivalent risk management frameworks. Given these exempt entities are required to comply with a comparable regulatory framework, relevant costs for meeting baseline compliance with the SOCI Act are already incurred, creating an existing regulatory cost base which does not need to be separately considered by this IA. Instead, the IA will consider the marginal uplift arising from the proposed reforms.

Regulatory cost per entity

The total regulatory cost estimate in the 2022 RIS was based on submissions from industry. The average regulatory cost estimate per submission for each critical infrastructure asset type is provided in Table 44.

Table 44 *Regulatory cost per entity from 2021-22 consultation (2022 base year)*[36]

	Cost ($ million)	*Cost ($ million)*
Critical infrastructure asset	Average one-off cost per entity (submissions)	Average annual ongoing cost per entity (submissions)
Critical electricity assets	8.1	3.8
Critical gas assets	10.5	2.1
Critical water assets	14.4	6.1
Critical data processing or storage assets	1.7	1.9
Critical broadcasting and domain name system assets	0.7	0.5

[36] These costs are presented as they were in the RIS 2022. They have not been indexed and are in 2022 base year dollars. However, these costs have been applied in the analysis in this IA. In considering the measures proposed in this IA, the regulatory costs presented here have been indexed to June 2024 based on the ABS CPI.

	Cost ($ million)	*Cost ($ million)*
Critical infrastructure asset	Average one-off cost per entity (submissions)	Average annual ongoing cost per entity (submissions)
Critical financial market infrastructure assets (payment systems)	0.1	1.4
Critical liquid fuels assets	8.9	2.6
Critical hospitals	13.0	10.1
Critical energy market operator assets	22.1	6.7
Critical freight infrastructure *and* critical freight services assets	3.9	2.3
Critical food and grocery assets	3.1	1.7
Total average cost per entity[37]	7.9	3.6

[37] For the purposes of this IA (and as referred to in the body of this document), these costs have been indexed to $8.8 million (average one-off cost per entity) and $4.0 million (average annual ongoing cost per entity).

Appendix B: Extract of Consultation Paper Questions

Note: The questions extracted below relate to the reforms considered in this IA only, and includes only the questions in the Consultation Paper which relate to the proposed reforms.

[Measure 1] Protecting critical infrastructure – Data storage systems and business critical data

- How are you currently managing risks to your corporate networks and systems holding business critical data?
- How can the proposed amendments to the SOCI Act address the risk to data storage systems held by critical infrastructure while balancing regulatory burden?
- What would be the financial and non-financial impacts of the proposed amendments? To what extent would the proposed obligations impact the ability to effectively use data for business purposes?

[Measure 2] Improving our national response to the consequences of significant incidents – Consequence management powers

- How would the proposed directions power assist you in taking action to address the consequences of an incident, such as a major cyber incident on your critical infrastructure asset?
- What other legislation or policy frameworks (e.g., at a state and territory level) would interact with the proposed consequence management power and should be considered prior to its use?
- What principles, safeguards and oversight mechanisms should Government establish to manage the use of a consequence management power?

[Measure 3] Enforcing critical infrastructure risk management obligations – Review and remedy powers

- How would the proposed review and remedy power impact your approach to preventative risk?

Appendix C: Consultation Questions & Summary of Industry Views on Draft IA

Consultation questions

[Question 1] Problem

- Is the problem set out above accurately described in relation to your entity? Are there other elements of the problem which have not been mentioned above?
- Do you have any key examples from your experience which demonstrate or mitigate the significance of the identified problem?

[Option 1] Status Quo

- Are the impacts of Option 1 accurately described as related to your entity?
- What do you consider would be the most material costs to your entity of Option 1?
- Are there any other impacts (negative, positive, or neutral) arising from the status quo which have not been mentioned above?

[Option 2] Legislative Reform

Measure 1: Protecting critical infrastructure – Data storage systems and business critical data

- Are the costs of Measure 1 accurately described as related to your entity?
- Will a requirement to capture 'business critical data' in your risk management activities have a material impact on staff effort, capital expenditure or operating costs? If so, what do you estimate will be the marginal cost increase for your entity?
- Are there any other impacts arising from Measure 1 which have not been mentioned above?
- Are the categories of costs identified above an accurate representation of the impact of a direction/s?
- Are there other scenarios which you foresee as arising under a consequence management power, and would like Government to consider in this IA?

Measure 2: Improving our national response to the consequences of significant incidents – Consequence management powers

- Are the costs of Measure 2 accurately described as related to your entity?
- What do you consider would be the most material costs to your entity of Option 2 (when considering any marginal impact on staff effort, capital expenditure or operating costs)?
- Are there any other impacts arising from Measure 2 which have not been mentioned above?

Measure 3: Enforcing critical infrastructure risk management obligations – Review and remedy powers

- Are the costs of Measure 3 accurately described as related to your entity?
- If issued a direction to rectify a deficient RMP, will there be a material impact on staff efforts, capital expenditure or operating costs? If so, what do you estimate will be the marginal cost increase for your entity?
- Were the RMP costs described in the 2022 RIS consistent with your actual costs to ensure compliance with your obligations under the SOCI Act?
- Are there any other impacts arising from Measure 3 which have not been mentioned above?
- Are the benefits of Option 2 accurately described as related to your entity?
- What do you consider would be the most material costs to your entity of Option 2?
- Are there any other impacts (negative, positive, or neutral) arising from Option 2 which have not been mentioned above?

[Option 3] Voluntary participation

- Are the impacts of Option 3 accurately described as related to your entity?
- What do you consider would be the most material costs to your entity of Option 3?
- Are there any other impacts (negative, positive, or neutral) arising from the Option 3 which have not been mentioned above?

Summary of industry views

Table 45 *Summary of industry views*

Proposal	Summary of industry views
Measure 1: Protecting Critical Infrastructure – Data systems and business critical data	Enhancing regulatory oversight could lead to a **more standardised approach to cybersecurity across critical infrastructure sectors** and may provide **clearer expectations** for entities. **Should not be required to register data storage systems** that hold business critical data as standalone critical infrastructure assets. Recommends that **ministerial rules be implemented** to require that all operators of critical infrastructure consider and implement **appropriate safeguards against the material risks to their business critical data** and associated hazards. Responsibility for **business critical data systems should be explicitly defined and sit with the entity** that has primary operational control over the systems
Measure 2: Improving our national response to the consequences of significant incidents – Consequent management powers	• Concerns about how the reforms will **interact with existing frameworks.** • Support exercising powers to better **coordinate a national response** to a threat or incident. • Concerns in relation to **specific direction** on how to mitigate a threat in the context of individual businesses. • Measure needs to be **carefully worded to extend the time period allowable** for government to use existing intervention measures. • Department should **consider the complexity and bespoke nature of the unique operating environment** of entities when considering the practical application of step-in powers. • The implications of this measure must be considered to ensure a step-in process is **valuable and not disruptive**.
Measure 3: Enforcing Critical infrastructure risk management obligations – review and remedy powers	• Could also impose **significant compliance costs**, reduce flexibility for entities to manage risks according to their specific circumstances, and potentially **stifle innovation due to more prescriptive requirements.** • Government should consider maintaining a **sector-driven and contextualised approach** to review and remedy powers. • The Department should **consider guidance materials on what may be considered 'seriously deficient'** in terms of triggering the proposed remedy powers. • **Collaboration** with industry is encouraged on **developing guidance** and focus on addressing only those areas that have a significant and material impact.