Australian Government
Department of Home Affairs

Regulation impact statement: a risk management program framework for critical infrastructure assets

Department of Home Affairs, Cyber and Infrastructure Security Centre

25 November 2022

Table of Contents

I. Executive Summary

I. Executive summary

Critical infrastructure is essential for Australia's social and economic prosperity, national security, and national defence, and facilitating the provision of essential services across Australia.[1] However, risks to Australia's critical infrastructure have evolved in recent years. These risks are inherently complex, and reflect factors including increased cyber connectivity and greater participation in, and reliance on, global supply chains to support the provision of essential services. As such, it is urgent and imperative that the Australian Government take steps to prevent or mitigate risks to public safety and confidence; threats to our economic security or Australia's international competitiveness; as well as provide for the continuity of Government and its services, all of which are vulnerable to critical infrastructure disruptions.[2]

The Department of Home Affairs (the Department) is focussed on driving an uplift in the security and resilience of Australia's critical infrastructure, and providing assurance to Government that Australia's critical infrastructure is being managed in a secure and resilient manner. This focus was initially reflected in the passage of the *Security of Critical Infrastructure Act 2018* (Cth) (SOCI Act), which sought to manage national security risks arising from foreign involvement in Australia's critical infrastructure assets.

The Security Legislation Amendment (Critical Infrastructure) Bill 2020 (SLACI Bill) was first introduced to Parliament in December 2020 and sought to amend the SOCI Act to include more sectors with increased obligations. It sought to expand coverage of the Act from four sectors (electricity, gas, water and ports) to eleven sectors (communications, financial services and markets, data storage and processing, defence industry, higher education and research, energy, food and grocery, health care and medical, space technology, transport and water and sewerage). It also sought to introduce positive security obligations for owners and operators of critical infrastructure, such as a register of critical infrastructure assets and mandatory cyber security incident reporting, as well as last-resort government assistance powers, and information gathering and directions powers for the Department of Home Affairs. These aimed to provide the government with a clearer picture of critical infrastructure ownership and control, as well as enhanced opportunities to assist industry with its cybersecurity resilience and incident response.

As part of the positive security obligations, the SLACI Bill also sought to introduce compliance with an all-hazards Risk Management Program (RMP) for particular critical infrastructure assets. This would require responsible entities for critical infrastructure assets to have and comply with an RMP that identifies each hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset, minimises the material risk of the hazard and mitigates the relevant impact of the hazard on the asset.

The regulatory impact of the SLACI Bill's positive security obligations (excluding the RMP obligations), Enhanced Cyber Security Obligations, and enhanced Ministerial Directions 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).

Following a review of the SLACI Bill by the Parliamentary Joint Committee on Intelligence and Security of the 46th Parliament (hereafter PJCIS), the SLACI Bill was split into two Bills as

[1] Critical Infrastructure Centre, 2015, pg. 1

[2] Critical Infrastructure Centre, 2015, pg. 1

recommended by the PJCIS; the *Security Legislation Amendment (Critical Infrastructure) Act 2021* (SLACI Act), which received Royal Assent on 2 December 2021, and the *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022* (SLACIP Act), which received Royal Assent on 1 April 2022. The SLACIP Act includes the positive security obligation requiring critical infrastructure assets to develop and maintain a RMP.

While the SLACIP Act outlines the broad requirements for the proposed RMP (outlined above), it also provides for the Minister for Home Affairs (the Minister) to make rules which outline more specific requirements for an organisation's RMP. The Department has committed to develop these rules through a process of consultation with key industry stakeholders, to:

- ensure that there are rules in place for each sector that will drive an uplift in the security and resilience of critical infrastructure assets; and
- assess whether there are existing regulations that meet the objectives of the RMP, to reduce regulatory burden where possible.

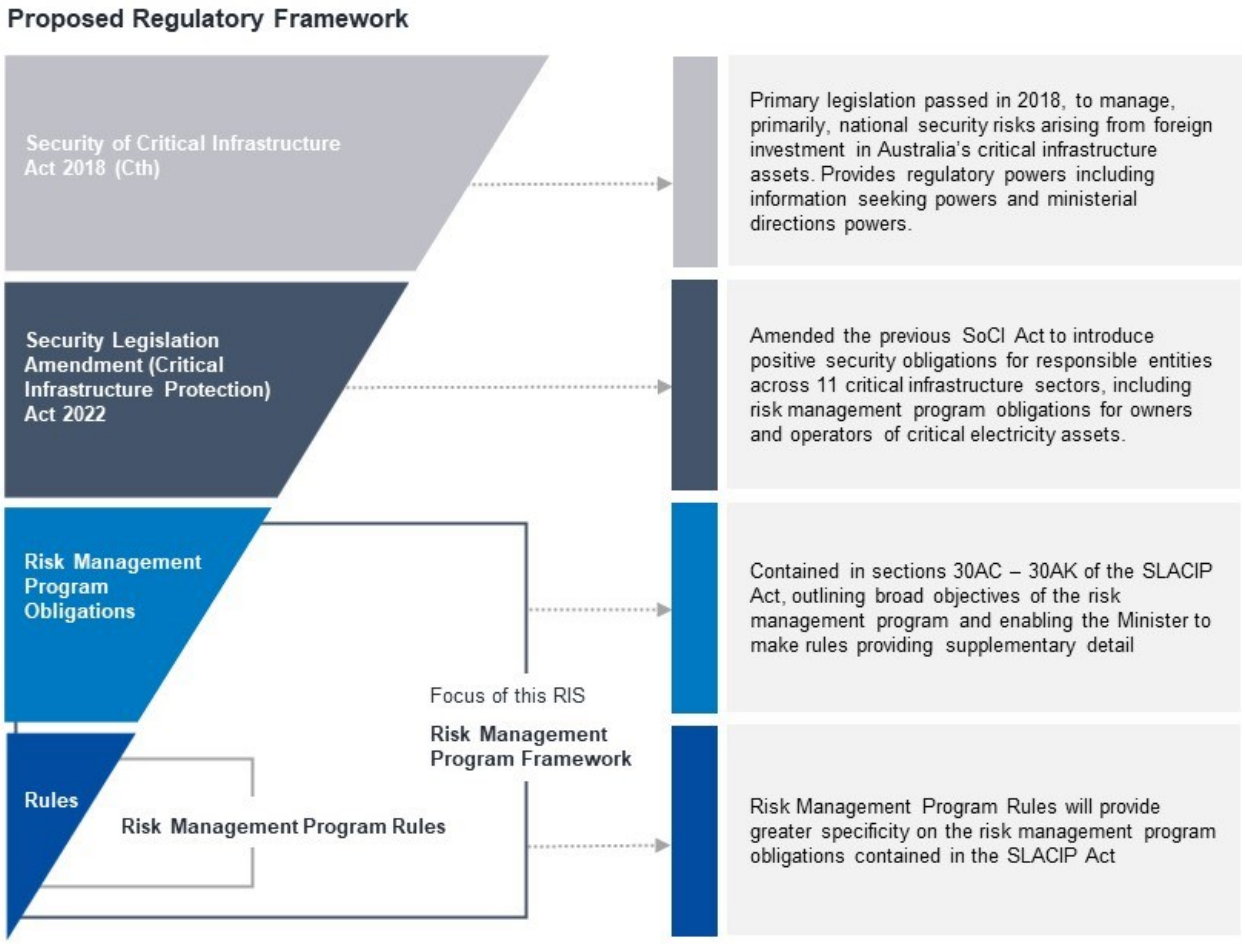
This RIS is focussed on the potential costs for the implementation of the RMP obligations that are set out in the SLACIP Act. These RMP obligations are underpinned by sector-agnostic RMP rules, for owners and operators of 13 critical infrastructure asset classes defined in the SLACI Act (referred to for the purposes of this RIS as 'relevant critical infrastructure asset(s)):

- critical electricity assets;
- critical gas assets;
- critical water assets;
- critical data processing or storage assets;
- critical broadcasting assets;
- critical financial market infrastructure assets (specifically payment systems);
- critical domain name systems;
- critical liquid fuels assets;
- critical hospital assets;
- critical energy market operator assets;
- critical freight infrastructure;
- critical freight services assets; and
- critical food and grocery assets.

The legal definition of each relevant critical infrastructure asset is contained in Appendices G – R.

The diagram below provides an overview of the proposed regulatory framework considered throughout this RIS, and the existing regulatory environment in which the SLACIP Act's RMP obligations, and proposed rules, would operate. For the purposes of this RIS, a reference to the RMP framework is a reference to the RMP obligations contained in the SLACIP Act, as well as sector-agnostic RMP rules, as indicated by the black box in Figure 1 below:

Figure 1: *Overview of proposed regulatory framework*



Terminology note: For the purposes of this RIS only, a reference to the RMP framework is a reference to the RMP obligations contained in the SLACIP Act, as well as sector-agnostic RMP rules, as indicated above in Figure 1.

In March 2021, the Department completed a consultation series with industry representatives from across the 13 critical infrastructure asset classes (outlined in the SLACI Act) and Government stakeholders to develop what were then referred to as sector-agnostic governance rules, which provide further specificity to the RMP requirements in the SLACIP Act. These are now captured in section 7 of the proposed RMP Rules as general rules[3]. For example, the general rules mandate how entities should identify hazards and risks for their RMPs and document activities for good risk practice within their organisation. Consultation for the RMP rules commenced with the electricity asset class in April 2021. This was followed by consultation with the Gas, Water and Sewerage, Data Storage or Processing, and Payment Systems asset classes between April and September 2021. The engagements with these asset classes, and the clear commonalities of approach to risk management identified during that engagement, directly informed the drafting of the RMP rules.

During a series of sector-agnostic town halls and sector-specific consultation sessions in October and November 2021, the Department consulted on the RMP rules with all critical infrastructure sectors for which the Department intends to propose to the Minister for Home Affairs to 'switch on' the RMP[4]. The Minister for Home Affairs commenced formal consultation on the Rules on 5

[3] Whilst now captured within the broader RMP Rules, references to general rules are made in this document, noting the RIS considered their specific impact.

[4] As per the SLACI Act and SLACIP Act, positive security obligations only apply where the Minister of Home Affairs has made either a rule or determination to 'switch on' the specific obligation for a specific critical infrastructure asset.

October 2022, with consultation open for 45 days to 18 November 2022. This consultation included two town-halls, four question and answer sessions, as well as specific engagement with the food and grocery asset class, following the decision to include them in the draft rules.

During these engagements the Department worked with sectors to refine the RMP rules, ensuring they are fit-for-purpose and achieve a baseline uplift in security. This RIS has been prepared to incorporate each asset class needing to adopt the RMP rules. Asset classes sit within critical infrastructure sectors and are defined according to the particular type of asset owned and operated, as defined in the SLACI Act.

This RIS argues that four problem elements exist in relation to critical infrastructure assets, which can be addressed through corresponding Government interventions, as outlined in Table 1 below:

Table 1 *Problems for critical infrastructure assets and Government objectives*

What is the problem for critical infrastructure assets?	What are Government's objectives?
There are growing risks to critical infrastructure assets. The RMP framework is required to ensure these growing risks are being considered and, where appropriate, addressed. This will enable the adoption of an all-hazards approach to risk management for critical infrastructure assets, increasing the resilience of these assets.	• **Lower the material risk** of hazards and the impacts of those hazards, as they manifest for critical infrastructure assets. • Ensure that adoption of the RMP for critical infrastructure assets is **reasonable and proportionate** to the purpose of the program.
Existing legislative arrangements are insufficient for the current threat environment. The RMP framework is required to provide specificity to the RMP proposed by the SLACIP Act and create a regulatory environment which seeks to address all hazard risks. Currently, there is no requirement for critical infrastructure entities to meet positive security obligations. Existing standards should be leveraged to minimise regulatory burden and duplication, and be enforced on a sector-wide basis.	• **Lower the material risk** of hazards and impacts of those hazards, as they manifest for critical infrastructure assets. • **Avoid regulatory duplication** and facilitate a **coordinated uplift** in responsible entities' compliance with relevant standards.
The Government has limited visibility of current risk management practices, and limited ability to ensure that risks are appropriately managed across sectors. The RMP framework will ensure risk management considerations are appropriately prioritised by responsible entities.	• **Improve Government's visibility** over the security and resilience of critical infrastructure assets. • Government will also have a range of graduated powers to **support an uplift** in resilience and security.
A stronger partnership between Government and industry is needed to drive a wholesale uplift in security and resilience. A strong and effective partnership between industry and Government is pivotal for ensuring the security and resilience of critical infrastructure is prioritised across all responsible entities. Consultation has drawn robust engagement from industry and recognition of Government's ability to regulate on matters of critical infrastructure in a meaningful manner.	• **Avoid regulatory duplication** and facilitate a **coordinated uplift** in responsible entities' compliance with relevant standards.

This RIS considers three options for addressing the above four problem elements – **option 1** involves maintaining the status quo (no regulatory change); **option 2** involves the implementation of, on a mandatory basis, a RMP framework for critical infrastructure assets, including supporting RMP rules; and **option 3** involves voluntarily implementing the RMP obligations contained in the SLACIP Act, as the obligation will not be 'switched on' for critical infrastructure assets. Additionally, this would include an option for industry to voluntarily comply with the RMP rules.

The analysis presented in this document clearly identifies that **option 2: mandatory RMP framework** most effectively addresses the identified problem areas, aligns with Government's objectives of protecting the essential services all Australians rely upon, and offers the greatest overall net benefit. For these reasons, the implementation of a mandatory RMP framework is the recommended course of action. However, this RIS seeks to analyse the three options, and their associated costs and benefits, two of which demonstrate the potential to achieve some or all the stated policy objectives, and one which maintains the status quo and therefore does not meet the stated policy objectives.

II. Introduction

II. Introduction

A. Purpose of this document

This RIS builds upon the regulatory impact analysis conducted in 2020 for the SLACI Bill. The SLACI Bill established the rationale for an uplift in risk management practices across identified critical infrastructure sectors; however, following the key recommendation of the PJCIS to split the SLACI Bill, this rationale will be applied to the SLACIP Act. This RIS examines the costs and benefits of implementing a RMP framework in accordance with requirements under part 2A of the SLACIP Act, and the RMP rules. The costs and benefits analysis also consider the uplift in risk management practices across Australia's critical infrastructure assets, and resultant cascading improvement in the security and resilience of interconnected critical infrastructure across Australia.

The analysis and discussion in this RIS have been informed by the information and draft rules available as of 13 December 2021, and *the Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 22/018) 2022*, issued 5 October 2022. Note: The two sets of rules are substantively unchanged.

Overview of the 2020 RIS

This RIS builds on the regulatory impact analysis conducted for the 2020 RIS. Table 2 Summary of 2020 RIS, in Table 2 below, indicates that the 2020 RIS assessed the regulatory impact of four measures and their burden on applicable critical infrastructure stakeholders:

***Table 2** Summary of 2020 RIS*

		2020 RIS: proposed regulatory measures		
		Positive Security Obligations*	**Enhanced Cyber Security Obligations**	**Ministerial Directions**
Affected Stakeholders	**Entities within 'Critical Infrastructure Sectors'**			
	As defined in Section 1.2 of the 2020 RIS and include, for example, the energy sector.			✓
	'Critical Infrastructure Assets'			
	Specific assets within critical infrastructure sectors, defined in the SOCI Act. For example, critical infrastructure assets.	✓		✓
	'Systems of National Significance'			
	Those systems declared by the Minister as most critical to Australia's social and economic stability, defence, and national security.	✓	✓	✓

Notes: *the 2020 RIS assessed the costs of complying with the Register of Critical Infrastructure Assets and cyber reporting obligation elements of the positive security obligations. It **did not** consider the costs of the RMP obligation element of the positive security obligations, which is addressed in this RIS.

The green shading above highlights the regulatory changes and subsequent regulatory burden analysed as part of the 2020 RIS. The grey shading indicates no regulatory change.

The 2020 RIS found that the implementation of legislative change was likely to have an annual aggregated cost to industry of $2.19 million, attributed to the Register of Critical Infrastructure Assets and the mandatory cyber incident reporting obligations in the SLACI Bill.

The costs associated with the Enhanced Cyber Security Obligations and the Ministerial Directions obligations do not require ongoing industry obligations and are upon request. Therefore, estimates were provided for the costs to individual entities if directed by Government to comply with a particular Enhanced Cyber Security Obligation or Ministerial Direction. These costs ranged from a $4,999 annual cost for compliance with a particular Ministerial Direction to a maximum annual compliance burden of $361,250 for a large system of national significance to comply with a telemetry enhanced cyber security obligation.

The 2020 RIS concluded the costs associated with the proposed regulatory changes were justified, as they would offer a substantial benefit in the form of increased security and resilience for Australia's critical infrastructure. It found that likely benefits of the legislative change included increases in resiliency, job creation, and a higher continuity in the provision of services to industry, businesses, and households.

The 2020 RIS considered the overarching costs and benefits of two elements of the positive security obligations: the reporting obligations to the Register of Critical Infrastructure Assets and

the mandatory cyber incident reporting obligation. This RIS analyses the regulatory impact of the RMP obligations (a subset of positive security obligations), and accompanying RMP rules for critical infrastructure assets.

Development of this RIS

The Department engaged with the Office of Impact Analysis (previously Office of Best Practice Regulation) throughout the policy development process. The regulatory impact statement was at the following stages of development at key decision points:

- Government approval – Draft
- Draft SLACIP bill exposure to Senior Officials and to the PJCIS – First pass
- Decision of Government on the Risk Management Program Rules – Second pass

B. What is 'critical infrastructure'?

The Commonwealth Government's Critical Infrastructure Resilience Strategy 2016 defines critical infrastructure as:

> *"…Those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation or affect Australia's ability to conduct national defence and ensure national security."*[5]

The introduction and passage of the SLACI Act reflects the Government's priority to provide greater clarity on the particular sectors defined as critical infrastructure sectors. Table 3 below lists the critical infrastructure sectors **relevant to this RIS**, and corresponding relevant critical infrastructure assets. Refer to Appendices G – R for further detail on the relevant critical infrastructure sectors.

Table 3 *Critical infrastructure sectors and asset classes*

Critical Infrastructure Sector	Relevant critical infrastructure assets
Energy	• Critical electricity assets • Critical gas assets • Critical liquid fuels assets • Critical energy market operator assets
Water and Sewerage	• Critical water assets
Data Storage and Processing	• Critical data processing or storage assets
Communications	• Critical broadcasting assets • Critical domain name systems
Financial Services and Markets	• Critical financial market infrastructure assets (specifically payment systems)
Health	• Critical hospitals
Transport	• Critical freight infrastructure assets • Critical freight services assets

[5] Critical Infrastructure Centre (2015), p. 1.

Critical Infrastructure Sector	Relevant critical infrastructure assets
Food and Grocery	• Critical food and grocery assets

This RIS is focused on entities who own or operate a critical infrastructure asset ('responsible entities'), as described in the *Critical Infrastructure (Definitions) Rules (LIN 21/039) 2021,* that is in one of the aforementioned asset classes.

The importance of critical infrastructure

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 economic prosperity and public safety would be threatened.

Existing critical infrastructure frameworks are being outpaced by an evolving threat environment. Natural hazards are increasing in prevalence, information technology and operational systems are converging, the complexity of cyber threats is growing, and foreign intelligence activities against Australian interests are increasing in frequency and sophistication.

The interconnected nature of critical infrastructure means that, without proper safeguards, deliberate or inadvertent disruption of one critical infrastructure asset can result in cascading impacts for Australia's social and economic stability, defence and national security. While owners and operators of critical infrastructure have strong incentives to ensure the resilience of their own assets to varying standards, the interconnectedness and significance of these assets warrants the application of consistent standards on a whole-of-sector basis.

C. Role of the SLACIP Act

Building on the existing requirements contained in the SOCI Act, the SLACIP Act introduces an enhanced regulatory framework for critical infrastructure sectors. This includes, most relevantly, additional positive security obligations for critical infrastructure assets, including compliance with RMP obligations outlined in sections 30AC – 30AKA of the SLACIP Act.[6] The benefits of the SLACIP Act, including its proposed RMP obligation, were highlighted in the 2020 RIS. The 2020 RIS also included an analysis of the qualitative impact of the (1) RMPs, and the qualitative and quantitative impact of (2) the register of critical infrastructure assets and (3) the notification of cyber incidents obligation.

The SLACIP Act acknowledges that entities are best placed to understand risks to their critical infrastructure assets and seeks to outline principle-based, rather than specific, outcomes. In relation to the proposed RMP obligations, section 30AH of the SLACIP Act provides:

(1) *A **critical infrastructure RMP** is a written program:*

- *(a) that applies to a particular entity that is the responsible entity for one or more critical infrastructure assets; and*
- *(b) the purpose of which is to do the following for each of those assets:*
  - *(i) identify each hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset;*
  - *(ii) so far as it is reasonably practicable to do so—minimise or eliminate any material risk of such a hazard occurring;*
  - *(iii) so far as it is reasonably practicable to do so—mitigate the relevant impact of such a hazard on the asset; and*

[6] *Security Legislation Amendment (Critical Infrastructure) Act 2021.*

(c) that complies with such requirements (if any) as are specified in the rules.

Section 30AA of the SLACIP Act provides that the purpose of a critical infrastructure RMP is for the responsible entity for critical infrastructure assets to do the following for each of those assets:

(a) identify each hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset;
(b) so far as it is reasonably practicable to do so—minimise or eliminate any material risk of such a hazard occurring;
(c) *so far as it is reasonably practicable to do so—mitigate the relevant impact of such a hazard on the asset.*

For industry, the RMP sets an expectation that they address all hazard risks to their critical infrastructure assets. It will support an uplift where those risks are adequately managed, provide consistency across identified critical infrastructure assets, and increase the resilience of both responsible entities of critical infrastructure assets and their downstream entities. For Government, the RMP increases visibility and offers assurance that critical infrastructure assets are appropriately managed. In the absence of market drivers, the RMP can support Government in facilitating industry-wide prioritisation and management of risks.

While the SLACIP Act sets out the overarching RMP obligations, it provides that more detailed requirements can be contained in rules. For critical infrastructure assets, the proposed rules would be categorised into the RMP rules (See Section 4).

D. Overview of the role of critical infrastructure assets in Australia

The following is a brief overview of critical infrastructure assets included in this RIS:

- The generation, transmission, distribution, and supply of **electricity** is a major contributor to Australia's economy and essential for the efficient conduct of almost all day-to-day activities. For 22 million Australians, electricity is provided by the National Electricity Market (NEM), covering the six eastern and southern states and territories, while Western Australia and the Northern Territory manage their own grids under separate regulatory arrangements.
- The production, processing, transmission, distribution, and supply of **gas** is a major contributor to Australia's economy and enables many day-to-day activities. There are three distinct gas regions in Australia, the East Coast region (including Queensland, New South Wales, Australian Capital Territory, Victoria, Tasmania, and South Australia), Western region (including Western Australia) and the Northern region (including the Northern Territory).
- Australia's critical **water** assets are an essential part of life and critical for the ongoing health and prosperity of Australia. Critical water assets can be categorised into water supply assets, including water catchment and bulk water supply services; water distribution assets, such as water reticulation systems; and sewage and drainage services, including water and sewage treatment plants and sewage network operations.
- **Data processing and storage** is an integral part of everyday life and commonly used by individuals, industry, and governments across Australia. Data storage and processing is key to the functioning of internet services, other digital services, the processing of payments, and the use of digital applications.
- The **broadcasting** sector of the communications industry is comprised of radio and television (free-to-air) sub-sectors, and plays a particularly important role in emergency management through the provision of forecasts and regular updates. Broadcast media also plays an important role in national campaigns, both in disseminating and collecting information.
- **Financial market infrastructures** deliver services critical to the smooth functioning of financial markets and financial stability. The smooth functioning of **payment systems** is important for economic activity, financial stability, and public trust.

- **Domain name systems** are critical for the functioning of Australian businesses, the Government, and the community, with disruptions having the power to compromise the users' ability to conduct business, navigate the internet, or access their data. The Australian '.au' namespace has over 3.2 million domain names registered as of August 2020.[7] Oversight of '.au' is provided by the .au Domain Administration (auDA), a not-for-profit organisation which operates under sponsorship from the Internet Corporation for Assigned Names and Numbers (ICANN), and is endorsed by the Australian Government.[8]
- Australia's economy is reliant on **liquid fuels** and will be for some time to come. Liquid fuels are a critical input into the mining, agriculture, transport, international tourism, and defence sectors.
- **Hospitals** are an important part of Australia's health care system and a crucial enabler of Australia's economic stability more broadly, as highlighted by the COVID-19 pandemic. Intensive care units (ICUs) are one of the most critically functioning operational environments in a hospital.
- **Energy market operators** are crucial to the functioning of electricity and gas systems and markets across Australia. The Australian Energy Market Operator (AEMO) manages most wholesale and retail electricity and gas markets nationally, including the National Energy Market (NEM), servicing over 22 million Australians across the six eastern and southern states and territories, and the (WEM) in Western Australia.
- **Freight infrastructure and services** form crucial parts of the supply chain for Australian imports, exports, and domestic consumption. Freight infrastructure provides critical corridors for the transportation of goods, while freight service providers conduct business that is essential to the transportation of goods.
- Access to **food and groceries** is a fundamental right for all Australians, recognised as such in the Article 11 of the *International Covenant on Economic, Social and Cultural Rights* (ICESCR).

[7] Critical Infrastructure Centre, 2021, p. 21

[8] auDA, 2021

1. What is the problem?

1. What is the problem?

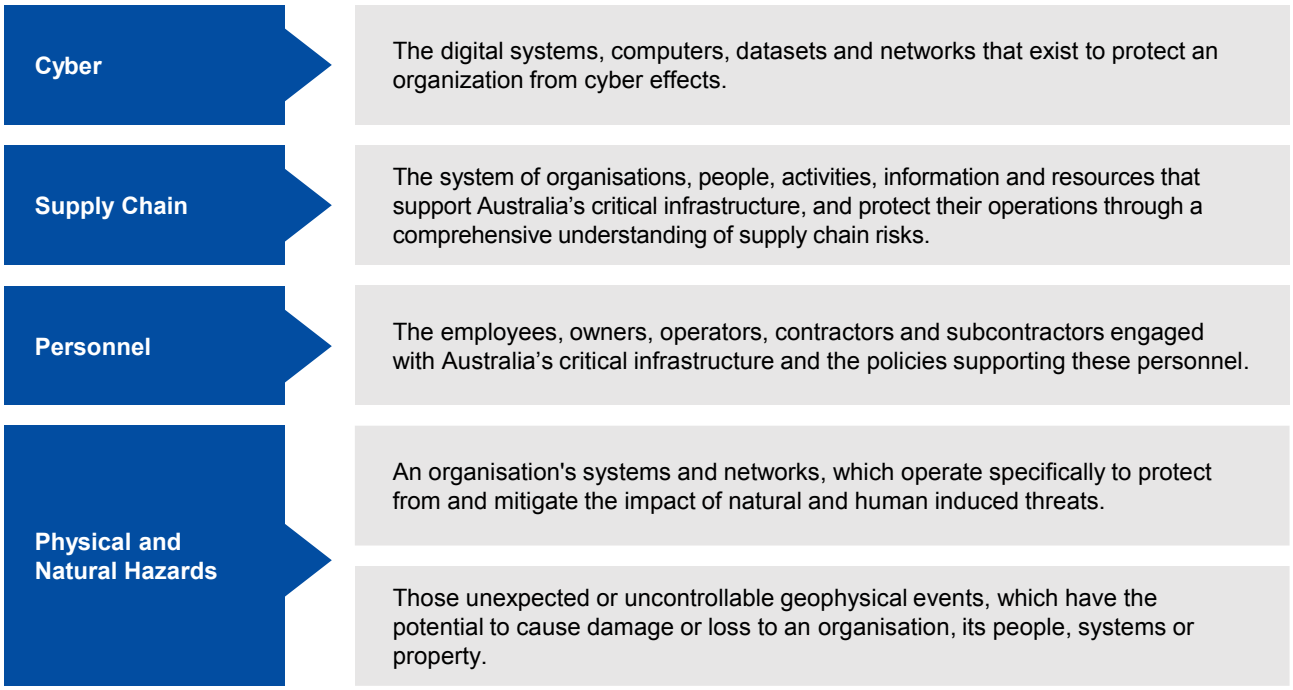
The interconnected nature of critical infrastructure assets, as well as their role in supporting the functioning of, and services provided by, other critical infrastructure sectors, intensifies the overall risk and subsequent impact of any disruption. To that end, there are four problem elements which currently exist for critical infrastructure assets, as described in Table 4. These are discussed in greater detail in Section 1.2 below.

Table 4 *Four problem elements for critical infrastructure assets*

Problem Elements	Recommended Solutions
1.2.1 There are risks to critical infrastructure assets.	The RMP framework is required to ensure these risks are being considered and, where appropriate, addressed. This will enable the adoption of an all-hazards approach to risk management for critical infrastructure assets, increasing the resilience of critical infrastructure assets.
1.2.2 Existing legislative arrangements are insufficient for the current threat environment.	The RMP framework is required to provide specificity on the RMP introduced by the SLACIP Act and create a regulatory environment which seeks to address all hazards & risks. The SOCI Act, following the passage of the SLACI Act and the Minister commencing associated rules, means that designated responsible entities across all relevant critical infrastructure assets were required to provide information to the Register of Critical Assets and comply with Mandatory Cyber Incident Reporting obligations. Existing standards should be leveraged to minimise regulatory burden and duplication and enforced on a sector-wide basis.
1.2.3 Currently, the Government has limited visibility of current risk management practices and limited ability to ensure risks are appropriately managed across sectors.	The RMP framework will ensure risk management considerations are appropriately prioritised by responsible entities. Government will also have a range of graduated powers to support an uplift in resilience and security across Australia's critical infrastructure assets.
1.2.4 A stronger partnership between Government and industry is needed to drive a wholesale uplift in security and resilience.	A strong and effective partnership between industry and Government is pivotal for ensuring the security and resilience of critical infrastructure is prioritised across all responsible entities. Consultation has drawn robust engagement from industry and recognition of Government's ability to regulate on matters of critical infrastructure in a meaningful manner.

The primary objective of critical infrastructure regulation is to improve critical infrastructure resilience and mitigate the potential impacts of 'all hazards'. The SLACIP Act's RMP requires industry to consider all hazards, which encompass natural and physical hazards (for example, fires, floods and cyclones, health hazards) and hazards related to people which may also affect supply chains (for example, unlawful interference, cyber incidents, espionage, chemical or oil spills, and trusted insiders). Without adequate protection, threats or hazards are likely to manifest within four key hazard domains (see Figure 2 below):

Figure 2: *Outline of four key hazard domains*



Risk management must be considered using an all-hazards approach to maintain the operation and reliability of Australia's essential services and ensure Australians' way of life is not disrupted or degraded by an event categorised under any one of the four hazard domains.

There are a range of potential consequences of a prolonged or widespread disruption to critical infrastructure, as illustrated by the following examples:

A prolonged disruption to **electricity** supply may result in disruptions to food and grocery supplies, water supply and sanitation facilities, telecommunications networks, transport infrastructure and financial services. Such a disruption occurred in May 2021 when the Callide Power Station, located in Queensland, was affected by an explosion; this left more than 470,000 customers without power for an afternoon until power was restored with support from other states, and with the help of renewables.[9] While damage to the power station itself was deemed 'catastrophic', the incident also had cascading effects for several other electricity generators and transmitters as well as for other sectors across Queensland, such as transport, food and groceries, water and sewerage.

A disruption or compromise of **water** supply could have potentially severe consequences for health, safety, and life itself. For example, in 2020, one of Queensland's largest water entities, Sunwater (who is responsible for managing 19 dams and approximately 40% of Queensland's commercial-use water) was the victim of a cyber-attack, which continued for nine months. The cyber-attack was conducted by threat actors with the intention to use IT infrastructure to direct bots to increase the amount of views on a particular YouTube video, for financial gain.[1] If the threat attackers had more malicious intentions, they had the opportunity to control operational systems, creating potential risks such as contamination of the Sunwater water supply, which could have exposed thousands to contaminated water causing sickness, severe illness, or possibly death.

Prolonged downtime of key **data storage or processing** assets could impact business operations across the economy, reducing business confidence and financial stability. It may also result in sensitive data loss, with potential legal ramifications, as well as the possibility of reputation damage. In November 2021 Frontier Software, one of Australia's largest software providers of payroll and HR services, was affected by a ransomware attack that left 330 employers without

[9] Pollard, 2021

automated payroll for four days, as the company was forced to take down its server following the encryption of its systems. The ransomware attack also resulted in a data breach affecting at least 38,000 South Australian Government employees, with a number of employee's personal details being published on the Dark Web.[10]

Further information on these, and other, examples of the impacts of disruption to each relevant critical infrastructure asset are contained in Appendices G – R.

1.1. Increasing threats, connectivity, and complexity of critical infrastructure

Threats to Australia's critical infrastructure are increasing in frequency and complexity. For example, there has been a notable increase in the realisation of cyber security risks across Australia. In the 2019 – 2020 reporting period, the Australian Cyber Security Centre (ACSC), responded to 2,266 cyber security incidents.[11] Of these, 36.5% were categorised as moderate incidents (involving scanning, reconnaissance, or low-level malicious attacks on Federal, State or Territory Governments, large organisations or supply chains), while 33.3% were considered substantial incidents (involving low-level malicious attacks, malware, exfiltration or deletion of sensitive data, or sustained disruption of essential systems for Federal, State or Territory Governments, large organisations, supply chains or essential services).[12] The 2019 – 2020 reporting period demonstrates a significant increase on the 671 cyber security incidents which warranted a response by the ACSC in the 2016 – 2017 reporting period.[13] The ACSC also noted in the report, 'Australia's Cyber Security Strategy 2020', that critical infrastructure providers were the victims of around 35% of reported cyber incidents perpetrated by malicious actors in the year until 30 June 2020. During the COVID-19 pandemic, the ACSC observed an increase in phishing campaigns and COVID-19 themed malicious cyber activity. On 19 June 2020, the former Prime Minister, the former Minister for Home Affairs and the former Minister for Defence released a statement that Australian organisations across a range of sectors, including essential service providers and operators of critical infrastructure, were being targeted by a sophisticated state-based cyber actor. The statement acknowledged that the malicious activity was not new, but the frequency was increasing.[14]

Since the 2017 WannaCry ransomware campaign, which affected some 230,000 individuals and over 300,000 computer systems in 150 countries, the ACSC reported an increase in the number of ransomware incidents against Australian organisations.[15]

Similarly, the Australian Security Intelligence Organisation's (ASIO) *2018-19 Annual Report* identified that Australia continues to be a prominent target for espionage and foreign interference. The report states:

> *'…foreign intelligence services seek to exploit Australia's businesses for intelligence purposes…[and] [t]hat threat will persist across critical infrastructure, industries that hold large amounts of personal data, and emerging sectors with unique intellectual property that could provide an economic or strategic edge'.*[16]

These concerns persist in the ASIO *2020-21 Annual Report*, which states:

---

[10] South Australian Government 2021

[11] Australian Signals Directorate July 2019 - June 2020, p. 6

[12] Australian Signals Directorate July 2019 - June 2020, p. 6

[13] Australian Signals Directorate 2017, p. 53

[14] The former Prime Minister of Australia, 2020

[15] Australian Signals Directorate, 2020

[16] Australian Security Intelligence Organisation 2018-2019

> *'Foreign powers and their proxies, including intelligence services, continue to steal proprietary, sensitive and commercially valuable Australian information …. The increasingly interconnected nature of Australia's critical infrastructure exposes vulnerabilities which, if targeted, could result in significant consequences for our economy, security and sovereignty.'*[17]

Moreover, in 2021 a newspaper article quoted Senator James Paterson, the then chair of the Joint PJCIS which undertook the review into the SLACI Bill (and the SLACIP Bill in March 2022), saying that '*independent experts before the committee say they believe it is likely there is already a dormant presence on some of those critical networks of a foreign state that could be activated in the event of a regional conflict or crisis.*'[18]

While, in some cases, initiatives such as the Notifiable Data Breaches Scheme (NDBS) managed by the Office of the Australian Information Commissioner (OAIC) compel captured organisations and agencies to report unauthorised access to or disclosure of personal data, limited compulsions exist in Australia for cyber security incidents. Agencies in the United States and United Kingdom estimate a gap in the millions, between the number of reported cyber security incidents and the number of incidents which actually occur and go unreported.[19]

In addition to the malicious activity perpetrated in the cyber domain, the COVID-19 pandemic revealed the need for an increase in resilience in the supply chains of critical infrastructure. The COVID-19 pandemic has highlighted Australia's reliance on particular parts of the world for essential goods and services, and has increased awareness of, and sensitivity to, supply chain risks. Fear of shortages led to panic buying and concerns as to how reliance on imports can jeopardise a country's ability to meet their populations' needs. Likewise, global economic adjustments, including decreasing resource prices and the exchange value of Australia's currency, increase the cost-competitiveness of Australian manufacturing and heighten the need to adequately protect domestic capabilities.[20]

The Commonwealth Scientific and Industrial Research Organisation (CSIRO) recognises that not only do climate and natural disaster events have 'shattering impacts across the nation', the risk of these events occurring in a convergent, consecutive and compounding manner is increasing.[21] Likewise, the Ecological Threat Register provides that, worldwide, there has been a tenfold increase in the number of natural disasters since the 1960s. 39 incidents were recorded in 1960, compared with 396 in 2019.[22] The CSIRO also acknowledges that existing emergency and disaster management practices are insufficient for addressing this growing risk:

> *"…Not approaching and addressing the weakest link causes people to get hurt. Properties are lost, infrastructure fails, and the environment is decimated…the best areas to focus on to improve disaster resilience and preparation are planning, prevention of impact, relief and long-term recovery [through] better integration and coordination."*[23]

Owners and operators of critical infrastructure, whether public or private, exist in a market environment characterised by growing interconnectivity and heightened reliance on technology. While such connectivity through technology offers efficiency and tangible economic benefits, it can present new vulnerabilities particularly when combined with an evolving, all hazard threat environment. Where vulnerabilities are exposed and threats are realised, the supply of essential

---

[17] Australian Security Intelligence Organisation, 2021, p. 19-20.

[18] Sunday Herald Sun, 2021

[19] Swinhoe 2019

[20] Australian Government Productivity Commission 2021

[21] Lyne 2020

[22] Vision of Humanity n.d.

[23] Vision of Humanity n.d.

services across Australia can be significantly compromised. Since 2020, globally, the COVID-19 pandemic demonstrated the rapid and widespread consequences of unanticipated disruptions, resulting in substantial security, social and economic implications. In Australia, delays in the delivery and distribution of a range of essential goods and services, as a result of supply chain and personnel disruption, resulted in significantly diminished product availability.

While it is imperative that critical infrastructure assets are appropriately secure, a sector is only as strong as its weakest link. It is not sufficient that a single asset has secure practices in place for all hazards threat protection. This is because a disruption to the operability of a critical infrastructure asset may impose significant implications on other critical infrastructure assets in the same sector, as well as for other critical infrastructure assets across other, interconnected sectors.

Past incidents, in both Australia and overseas, demonstrate the potentially severe, cascading consequences of prolonged disruption in any critical infrastructure sector – for that sector itself, for other critical infrastructure sectors, and for the affected national economy. The following case studies are three severe examples of a disruption of critical infrastructure in the gas, data, and liquid fuel sectors. Each are categorised by its relevant hazard domain(s). While some are drawn from overseas, these case studies highlight a clear imperative for decisive action, to prevent the occurrence of similar, or further, incidents for Australia's critical infrastructure assets.

Former Employee Attacks Cisco Systems (2018)	Personnel Risk
Situation: In September 2018, a former Cisco employee accessed Cisco Systems' cloud infrastructure, hosted by Amazon Web Services, without Cisco's permission. The former employee admitted that during his unauthorized access he was successful in deleting 456 virtual machines for Cisco's WebEx Teams application, which provides video meetings, video messaging, file sharing, and other collaboration tools.[24]	
Outcome: The former employee's actions caused more than 16,000 WebEx Teams accounts to be shut down for up to two weeks. Cisco was forced to spend approximately $1.4 million USD in employee time to restore the damage to the application and refund over $1 million USD to affected customers. No customer data was compromised as a result of the attack. The perpetrator was sentenced to 24 months in prison and ordered to pay a fine for intentionally accessing a protected computer without authorisation and recklessly causing damage.[25]	
Identified Gap: This case study demonstrates the need to screen and maintain awareness of the potential threats posed by current and former employees of critical data assets. This incident highlights the financial impediments and compromised personal data risks which may arise where insufficient employee checks are undertaken, user access is not appropriately controlled, and off boarding processes are not sufficiently rigorous.	

Cyber Attack Shuts Down U.S. Fuel Pipeline System (2021)	Cyber & Supply Chain Risk
Situation: A cyber-attack allegedly conducted by a criminal network on the Colonial Pipeline, an 8,850km pipeline which carries almost half of the fuel consumed along the U.S. East Coast, forced the Pipeline's closure for almost a week. Although the infiltration immediately affected the Pipeline's business computer systems (rather than the systems which run the pipelines), the pipelines' closure was a necessary precaution while investigations were undertaken. The incident is thought to be the largest cyber-attack on oil infrastructure in the U.S.'s history.[26]	
Outcome: The pipelines' shutdown reduced the short-term availability of fuel, forcing fuel prices to climb and refiners to reduce production levels, as they had no means of distributing the gas. Consumers rushed to gas stations and engaged in 'panic buying', exacerbating shortages, and contributing to price increases. In the first two hours following the attack, more than 100GB of data was stolen. On 13 May 2021, it was reported that Colonial Pipeline paid a ransom demand of close to $5 million USD in order to obtain a decryption key from the hackers responsible for the attack.[27]	
Identified Gap: The attack highlighted the need for entities to maintain pace with evolving malware capabilities and work to strengthen their 'last line of defence'. Chainalysis, a US cyber-security firm, suggests the amount paid in Bitcoin ransoms increased by 311% in 2020 (compared with 2019), to approximately $350 million (USD).[28] Without adequate protections and consistent re-evaluations, operating systems may be compromised.[29] It also highlights that while it is imperative to ensure the protection of critical gas assets, supplementary and connected services must also be preserved.	

ABC's south coast transmitter – Australia's summer bushfires	Physical and natural hazard
Situation: The Australian bushfires that devastated the South Coast of New South Wales (NSW) in the summer of 2020 caused widespread devastation and panic and, as the ABC's transmitter in the region	

[24] United States Department of Justice, 2020

[25] Ibid

[26] Gonzalez, 2021

[27] Osborne, 2021

[28] The Economist, 2021

[29] Volz, 2018

melted, communications with residents in the community were impaired by the inability to receive or transmit radio coverage.[30]

Outcome: It took months of repair work before the transmitter was completely operational again. The cost of restoring the infrastructure owned by BAI Communications Australia, which provides the broadcast towers to ABC on a commercial arrangement, was between $1.5 million and $2.0 million.[31]

Identified Gap: The ABC's managing director stated that the burn out damage demonstrates the critical necessity for AM radio technology, and that a backup generator should be maintained and in full operation to assist in getting information out during disasters like these. The analysts have been adamant that it is crucial that future infrastructure is as resilient as possible as broadcast towers still remain the weakest link during emergency broadcasts.

These examples clearly demonstrate the severity of consequences for any disruption to critical infrastructure assets, and the need to take proactive action to enhance their security and resilience. Case studies for each relevant critical infrastructure asset are contained in Appendices G – R.

1.2. The problem for critical infrastructure assets

There are four problem elements that relate to critical infrastructure assets summarised in Table 1 and Table 4 above. Collectively, these elements demonstrate the need for regulation to operationalise the objectives of the RMP obligations contained in the SLACIP Act.

1.2.1. Hazards create risks to critical infrastructure assets.

Hazards create risks to critical infrastructure assets, if realised, these risks have the potential to cause significant disruption across the Australian economy.

Hazards are categorised in four domains: cyber and information, personnel, supply chain, and physical and natural. For each relevant critical infrastructure asset, key hazards and the associated domain are summarised in Appendices G – R.

1.2.2. Existing legislative arrangements are insufficient for current threat environment.

There is significant existing regulation that will apply to responsible entities for critical infrastructure assets, including those outlined in Table 5 below. Responsible entities in all relevant sectors follow established risk management practices across several hazard vectors and comply with regulatory requirements under both federal, state and territory level regulation.

However, there are no legislative arrangements in place which impose a baseline all-hazard risk management requirement on responsible entities for critical infrastructure assets. The SLACIP Act, including through the RMP, will make a significant contribution towards improving all-hazard risk management across critical infrastructure assets, to uplift Australia's resilience and deter attacks on Australia's critical infrastructure.

The RMP rules, developed through consultation with industry stakeholders, will ensure the SLACIP Act's objectives are both sufficiently met and fit-for-purpose for industry. The Department worked with stakeholders to understand existing risk management practices within each sector, including identifying existing regulators, reporting requirements and potential regulatory gaps. Together, the Department and industry worked to address those gaps by developing RMP rules to achieve the desired security outcomes under the SLACIP Act. These rules draw on existing domestic and international frameworks and good risk management practices, based on academic and industry expertise. They provide strong baseline principles and standards to be built upon in the future.

[30] Lauder, Reardon, McCutcheon 2020

[31] Ibid

Existing critical infrastructure legislation

There are a range of legislative frameworks in place that seek to uplift critical infrastructure assets against some aspects of all hazard threats. Existing Commonwealth legislation that applies to critical infrastructure issues is outlined in Table 5 below. The table also highlights why existing regulatory schemes are not capable of addressing the problems discussed in this section.

***Table 5** Overview of Commonwealth critical infrastructure legislation*

Overview of regulation		Identified gaps
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.	Without the RMP obligations contained within the SLACIP Act 'switched on', the SOCI Act does not impose uplifted security obligations on critical infrastructure assets. Requirements on industry are limited and do not mandate active security and resilience management. While the Register of Critical Infrastructure Assets is invaluable to understand the aggregate picture of ownership and operation across Australia, it does not facilitate all hazard risk management.
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 inability of Government to impose requirements on entities to protect their assets has created an over-reliance on the FATA to manage risks. As the geopolitical environment continues to evolve, and Australia's national economy and critical infrastructure become ever more complex and interconnected, it is essential that the foreign investment review framework as set out in the FATA and the risk management framework under the SOCI Act adapt to meet these challenges. The SLACIP Act seeks to compliment the FATA by providing an ownership agnostic risk management framework.
Security Legislation Amendment (Critical Infrastructure) Act 2021	Established an enhanced framework for managing cybersecurity risks to an expanded list of 'critical infrastructure assets' by, among other mechanisms, creating a Register of Critical Infrastructure Assets and Government Assistance powers.	The SLACI Act does not impose all hazard risk management obligations on critical infrastructure assets.
Security Legislation Amendment (Critical Infrastructure Protection) Act 2022	Established the ability to designate the most important critical infrastructure assets as systems of national significant and apply enhanced cyber security obligations to these assets. Introduced critical infrastructure risk management program obligations to require all hazards risk management for certain assets.	The SLACIP Act does not impose all hazard risk management obligations on critical infrastructure assets without the risk management program obligations switched on by the Minister for Home Affairs.

Existing legislation related to each relevant critical infrastructure asset

In addition to Commonwealth legislation which applies to critical infrastructure, there are a range of sector-specific federal, state and territory legislative and regulatory frameworks which impose some obligations on responsible entities for critical infrastructure assets.

Refer to Appendices G – R for an overview of legislation and corresponding gaps which relate to each of the relevant critical infrastructure assets. Regulatory regimes which were not considered relevant for the purposes of this RIS, as they did not contain provisions pertaining to security or risk management, were not included for consideration.

There are several standards, guidelines and regulators which relate to each of the relevant critical infrastructure assets at a federal, state and territory level. An overview of these can also be found in Appendices G – R for each relevant critical infrastructure asset.

The legislative mechanisms and subsequent gaps highlighted indicate the growing need for greater preservation of Australia's critical infrastructure on a regulatory level. There is significant momentum and appetite for direction in the critical infrastructure space, as well as for critical infrastructure assets specifically. However, existing regulatory mechanisms either seek to address critical infrastructure security and resilience on a broad basis, with little or no reference to the nuanced operating environment of each critical infrastructure sector and its assets, or they do not impose obligations on a whole-of-sector basis, allowing for vulnerabilities in often highly interconnected sectors. This is not unexpected, as it is generally the role of delegated legislative instruments, such as rules, to capture and address unique industry and supply chain circumstances.

1.2.3. Currently, the Government has limited visibility of current risk management practices and limited ability to ensure risks are managed appropriately across sectors.

Existing legislative regimes do not provide the Government with adequate visibility of threats across the breadth of Australia's critical infrastructure assets. The majority of critical infrastructure assets are owned or operated by the private sector. Therefore, Government may have limited awareness of all hazard threats impacting critical infrastructure assets.

Without incentives to provide awareness to Government over the management and operation of critical infrastructure assets, nor the ability of market forces, in all instances, to correct this behaviour, Government has little power to assist in the event of threats such as cyber security incidents, if it is not requested by the affected entity. This can result in delays that substantially impact the provision of an essential service and hinders Government's ability to assist in resolving an incident, especially when dealing with time sensitive matters.

1.2.4. A stronger partnership between Government and industry to drive a wholesale uplift in security and resilience.

It is necessary to address vulnerabilities across all hazards which have the potential to affect critical infrastructure assets. This view appears to be strongly held by many segments of the community, as demonstrated in consultation for the Cyber Security Strategy 2020 where industry indicated that further engagement with, and direction from, Government would be useful for ensuring the protection of Australia's critical infrastructure.

There is a clear imperative to empower Government to:

- safeguard critical infrastructure assets against increasingly complex all-hazards risks through increased industry responsibility;
- manage these risks collaboratively with industry through strengthened engagement and a more structured relationship with the owners and operators of critical infrastructure assets; and
- respond rapidly in exceptional circumstances by making it clear what the Government is authorised to do.

Previous consultation on these issues has facilitated a stronger partnership between Government and industry, resulting in broad support for the introduction of an enhanced framework to secure critical infrastructure. Consultation on the reforms contained in the SLACIP Act was conducted between August and December 2021, through six virtual town halls (attended by 620

representatives from business and civil society), 22 virtual workshops (attended by 949 individuals) and 194 submissions in response to the 'Protecting Critical Infrastructure and Systems of National Significance' Consultation Paper.

Submissions were also received in response to a publicly released exposure draft of the SLACI Bill 2022 (which included the RMP components). Responsible entities for critical infrastructure assets such as the New Payments Platform stated that it 'supports the Government's policy objective of provision of direct assistance to private sector entities on critical cyber matters and positive security obligations for operators of critical assets.'[32]

Further, industry consultation on RMP rules has been completed with all relevant sectors. Through targeted and consistent engagement across a series of workshops, industry's awareness and understanding of the need to uplift the security and resilience of critical infrastructure assets has been enhanced. Consultation with industry indicated that responsible entities for relevant critical infrastructure assets often have mature risk management practices in place aligned to globally recognised standards. However, industry recognised the highly interconnected nature of critical infrastructure asset classes and sectors, as well as the increasing risks to critical infrastructure, necessitates a coordinated all-hazards approach to security and resilience from Government and industry.

For further consultation insights and stakeholder feedback received during the consultation process, see Section 5.

Industry's desire to strengthen its relationship with Government in the critical infrastructure realm aligns with one of the Critical Infrastructure Resilience Strategy's key outcomes – to achieve a strong and effective business-government partnership.[33] While existing resources, including the Strategy and the Trusted Information Sharing Network (TISN), make a substantial contribution to ensuring the continued, uninterrupted operation of critical infrastructure assets, these should be leveraged to generate a whole-of-sector focus on all hazard risk management.[34]

[32] Department of Home Affairs, 2020

[33] Critical Infrastructure Centre, 2015

[34] Critical Infrastructure Centre, 2015

2. Requirement for Government Action

2. Requirement for Government Action

2.1. Why should Government intervene?

Section 1 has highlighted that existing regulatory frameworks (see section 1.2.1) and market forces (see section 1.2.3) do not protect critical infrastructure against all hazard threats in a consistent and coordinated manner across critical infrastructure assets. Government, and its unique ability to regulate across supply chains and on a whole-of-sector basis, is capable of intervening to ensure vulnerabilities in critical infrastructure assets are proactively detected, prevented, and resolved. This is imperative for mitigating the potential impacts of disruption on Australia's social and economic stability, defence, and national security, as well as the reliability and security of other critical infrastructure assets.

Government, through the operation of various Departments, holds primary responsibility for national defence and security. It has existing and direct regulatory oversight of several critical infrastructure sectors and assets including communications, offshore oil and gas, banking and finance, and aviation.[35] Government's existing involvement in regulating Australia's critical infrastructure facilitated a comprehensive triaging process to identify sectors where existing regulatory arrangements do not meet the obligations contained in the proposed RMP.

The RMP element of the positive security obligations does not automatically apply upon commencement of the SLACIP Act. Instead, the Minister for Home Affairs is required to make rules to apply these obligations in relation to specific assets ('switch-on') following consultation with industry. This ensures Government considers the appropriateness of existing regulatory arrangements, and only applies the obligations in the Act once satisfied that existing arrangements are ineffective or insufficient.

This 'switch-on' mechanism is intended to prevent regulatory duplication in sectors where appropriate risk management arrangements already operate. For those sectors, the proposed RMP framework will not be switched on.

Government has several established mechanisms for industry engagement and compliance, which support the case for Government's continued intervention, including the following:

- The **Critical Infrastructure Resilience Strategy** is comprised of a policy statement and a plan, to support practical implementation of the critical infrastructure reforms in the SLACI Act and SLACIP Act. The Strategy aims to ensure the continued operation of critical infrastructure in the face of all hazards, including through outlining the ways in which changes in the critical infrastructure operating environment may impact the security and resilience of Australia's critical infrastructure, and outline key actions to be delivered under the Strategy.[36] The Strategy is currently undergoing an update, with a new version scheduled for release in 2022.
- The **Trusted Information Sharing Network (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. The TISN is designed to ensure the ongoing operation of critical infrastructure in the face of all hazards.[37]

[35] Critical Infrastructure Centre, 2015

[36] Department of Home Affairs, 2020

[37] Critical Infrastructure Centre, n.d.

- The establishment of the **Cyber and Infrastructure Security Centre (CISC)**, responsible for identifying and managing risks to Australia's critical infrastructure, indicates Government's commitment to working with its governing counterparts, as well as owners and operators of critical infrastructure assets, to ensure appropriate identification and management of risks.

Further, Government's continued involvement in critical infrastructure matters, as a co-designer and oversight authority for the RMP framework, aligns with each of the key outcomes identified in the Critical Infrastructure Resilience Strategy including:

1. A strong and effective business-government partnership;
2. Enhanced risk management of the operating environment;
3. Effective understanding and management of strategic issues; and
4. A mature understanding and application of organisational resilience.[38]

These key outcomes broadly align with Government's objectives identified below in Section 2.2. This alignment indicates that by intervening to consult with industry and implement supplementary rules to operationalise the objectives of the SLACIP Act's RMP framework, Government will be closer to achieving the above goals outlined in the Resilience Strategy, in addition to securing a whole-of-sector uplift in asset security and resilience.

2.2. Government's objectives

There are several specific objectives for Government intervention, aligned with the four problem elements identified in Section 1. These are outlined in Table 1 above in the executive summary.

With these objectives in mind, three policy options have been formulated. Each of these are discussed in detail in Section 3.

[38] Critical Infrastructure Centre, 2015

3. Policy Options

3. Policy Options

Three options have been considered in response to the identified problem elements:

- **Option 1**: Maintain the status quo;
- **Option 2**: Implement, on a mandatory basis, the RMP framework (encompassing the SLACIP Act's RMP obligations, underpinned by the RMP rules) which is legally enforceable against captured critical infrastructure assets;
- **Option 3**: Industry can voluntarily implement the SLACIP Act's RMP obligations, which will not be switched on for critical infrastructure assets. They can also voluntarily comply with the RMP rules.

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

3.1. Option 1: Maintain the status quo

Option 1 involves no regulatory action or legislative change as it applies to the RMP obligation. The RMP obligations in the SLACIP Act are not switched on for critical infrastructure assets.

Responsible entities would not be required to comply with the requirements contained in sections 30AC – 30AKA of the SLACIP Act. Neither these RMP obligations, nor the draft RMP rules, would apply for responsible entities of critical infrastructure assets.

Existing legislation, regulation, standards, and guidelines relating to critical infrastructure assets (set out in Appendices G – R) would remain.

3.2. Option 2: Mandatory RMP framework

Option 2 involves the requirement for industry to comply with a mandatory RMP. The RMP obligation of the SLACIP Act would be switched on for critical infrastructure assets.

It should be noted that the Department has closely examined the existing legislative and regulatory arrangements currently in place across all Australian jurisdictions. Information gathered during this assessment has been used to identify those sectors in which current risk management practices are insufficient for protecting the security and resilience of critical infrastructure assets. The measures proposed under option 2 would only be implemented where the Department has determined that existing measures are inadequate, in order to reduce risk of regulatory duplication. A summary of existing legislation and regulation that applies to specific sectors and assets, and identified gaps in terms of risk management obligations, can be found in Appendices G – R.

3.2.1. RMP obligation

Responsible entities would be required to comply with the requirements contained in sections 30AC – 30AKA of the Act and summarised in section 30AA:

- *The responsible entity for one or more critical infrastructure assets must have, and comply with, a critical infrastructure RMP.*
- *The purpose of a critical infrastructure RMP is to do the following for each of those assets:*
  (a) identify each hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset;
  (b) so far as it is reasonably practicable to do so—minimise or eliminate any material risk of such a hazard occurring;
  (c) so far as it is reasonably practicable to do so—mitigate the relevant impact of such a hazard on the asset.

- *A responsible entity must give an annual report relating to its critical infrastructure RMP. If the entity has a board, council or other governing body, the annual report must be approved by the board, council, or other governing body.*

These obligations would be supplemented by the **RMP rules**, including **general rules** which provide further specificity to the RMP requirements in the SLACIP Act; **standards and principles rules**, which seek to leverage existing best-practice standards related to critical infrastructure assets or include principles-based approaches to managing risk; and **material risk rules**, which may specify certain risks as 'material risks'.

The RMP framework would be binding and legally enforceable, with responsible entities facing civil penalties for non-compliance. The Department's approach to enforcement is discussed in greater detail in Section 7.1.3 below.

3.2.2. RMP rules

General rules

There is a need to support Government visibility over all hazards risk management, through implementing rules which require an entity to develop a RMP. Consultation on the manner and form of the (then) governance rules highlighted five key areas for coverage:

Risk methodology: The Department identified the need for a rule which requires an organisation's RMP to set out the risk management framework, which will support the organisation's development of an RMP. This rule stems from an acknowledgement that industry is best placed to identify, assess and manage risks to their business, and a need to provide further detail on risk management methodology outlined in the Act.

Context identification processes: The Department identified the need for a rule which requires an organisation's RMP to set out how it will carry out the following three context identification processes to assist with risk identification, as well as the outcomes of those processes.

a. Consider the components of the organisation which comprise critical infrastructure assets and the organisation's objectives. Some organisations may determine that some parts or components of an organisation are not essential for the functioning of the asset, or to meet business objectives.

b. Consider the types of relevant impacts that are of the greatest significance to an organisation's critical infrastructure assets. For example, an electricity generator may have greater concern as to availability rather than confidentiality, while a telecommunications provider may need to balance availability, confidentiality, and integrity risks equally.

c. Consider the interdependencies of an organisation's assets with other critical infrastructure assets.

Risk identification: The Department identified the need for rules which require an organisation's RMP to outline how risks will be managed in a holistic manner. Although the four main hazard domains (cyber, personnel, supply chain, and physical and natural hazards) are not mentioned expressly by the SLACIP Act, industry engagement has indicated that many organisations conceptualise their operations in these categories. Moreover, industry emphasised the need to ensure visibility of mitigations across each of these domains.

Accountability: The Department identified the need for rules which require that an organisation's RMP outline the individuals accountable for the respective elements of the RMP, as well as the person or persons who bear ultimate responsibility. The program's success relies on the appropriate allocation of responsibilities and accountabilities to ensure a clear, robust, and defensible program, and an evidenced commitment to good corporate social responsibility.

Reviews and updates: The Department identified the need for a rule which requires an organisation's RMP to outline the process by which the program will be reviewed regularly and kept up to date. The SLACIP Act requires that the program is reviewed on a regular basis.

Based on these five key areas, several general rules have been proposed (See Appendix E).

Standards and principles rules

In drafting RMP Rules, consideration of existing regulatory frameworks, including State and Territory legislation, was prioritised to avoid unnecessary regulatory duplication. Where rules require an entity to comply with a standard, flexibility has been provided to allow entities to identify standards they will comply with, which may allow for the use of standards already used by the entity.

Standards rules require that an entity's RMP refers to a specific standard across some or all of the identified hazard domains. Standards rules may leverage existing frameworks and standards, including maturity assessments, domestic standards, and international standards.

The Cyber and Information Security Hazards Rule domain is the only part of the current RMP rules, where a standard is proposed. Simplified, the rule can be expressed as:

*Responsible entities for critical infrastructure assets **must**, within **18 months** of the commencement of this rule, ensure that their risk management program includes details of how the responsible entity complies with at least one of the following standards and frameworks:*

a. The Australian Cyber Security Centre's Essential Eight Maturity Model at maturity level one;
b. AS ISO/IEC 27001:2015;
c. The National Institute of Standards and Technology (NIST) Cybersecurity Framework;
d. The Cybersecurity Capability Maturity Model (C2M2) at Maturity Indicator Level 1;
e. Security Profile 1 of the Australian Energy Sector Cyber Security Framework; or
f. an equivalent standard.

Standards rules require entities to structure their risk mitigation activities on a standard or framework. This approach supports comprehensive, coordinated, and complementary risk mitigation activities and ensures the effectiveness of responsible entities' RMPs.

Principles rules allow for businesses to continue to manage their own risks in the way that works best for their context and leverages existing risk management processes, whilst still providing assurance that security outcomes are achieved. The majority of the RMP Rules are principles-based, to support industry flexibility.

Examples of legislation, regulation and standards which were considered or referred to in the RMP Rules are contained in Appendices G – R for each relevant critical infrastructure asset. The current draft RMP Rules are in Appendix E.

Material risk rules

The SLACIP Act provides that the Minister for Home Affairs may make rules specifying a risk as a 'material risk'. Material risk rules will require entities to document, in their RMP, their holistic approach to the management of identified material risks. An entity must outline how it will consider the relevant impact of identified material risks on their assets, and how it will mitigate or minimise these risks across their organisation.

An example of a material risk rule that is included in the draft rules is:

*"Recognising the operating context differs between entities, when considering if a risk is a **material risk**, a risk management program should have regard to consideration of:*

a. impairment of a critical infrastructure asset that may prejudice the social or economic stability of Australia or its people; the defence of Australia or the national security of Australia"

The current draft material risk rules are contained in Appendix E, within the RMP Rules.

Material risks specified by rules will not amount to an exclusive, nor exhaustive, list. Responsible entities will be required to consider any and all material risks that may impact the confidentiality, availability, reliability, and integrity of their critical infrastructure assets.

3.3. Option 3: Voluntary RMP and guidance

Under option 3, the objectives of the SLACIP Act, including its proposed RMP obligations, would come into force through amendment to the SOCI Act. However, under option 3, the RMP obligation of the SLACIP Act would not be switched on for critical infrastructure assets. Responsible entities would not be required to comply with the requirements outlined in sections 30AC – 30AKA of the SLACIP Act, but could voluntarily choose to comply with these requirements.

In addition to voluntarily complying with the SLACIP Act's RMP obligations, responsible entities would also have an opportunity to comply with supplementary guidance.

The guidance would be based on the rules described above in Section 3.2 and grouped into two broad categories:

1. **Overarching guidance**, which are sector-agnostic and advise on matters of risk methodology, context identification processes, risk identification, accountability, reviews, and updates.
2. **Sector specific guidance material**, providing further advice on how an entity can comply with the RMP rules, including reference to specific standards or frameworks used in a sector across some or all of the identified hazard domains.

4. Likely net benefit of each option

4. Likely net benefit of each option

This section outlines the costs and benefits associated with the options considered in this RIS, in order to determine the likely net benefit of each option. The RIS considers the quantitative costs and benefits associated with option 2 (mandatory RMP framework) only, using a breakeven analysis. Qualitative costs and benefits have been included to supplement this analysis. For option 1 (maintain the status quo) and option 3 (voluntary RMP and guidance), qualitative costs and benefits were considered, with some inclusion of quantification where possible. As such, this section outlines the costing methodology used to determine the costs associated with option 2 only.

4.1. Net benefit methodology: Option 2

Following the completion of the RMP consultation process, a methodology was developed to determine the net benefit associated with option 2. The methodology is outlined in Table 6 below. Steps 1-4 detail the methodology for estimating costs, Step 5 indicates the process for determining benefits, and Step 6 establishes the methodology for conducting the net benefit analysis.

Table 6 *Option 2 costing methodology*

Step	Description
1 **Develop and validate costing approach with industry.**	Overview of costing approach The costs to industry of the proposed RMP framework were developed based on submissions from individual responsible entities on the costs to their organisation (Steps 2-3). The total cost for all critical infrastructure assets was then extrapolated from the responses received (Step 4). Basis for cost estimations **Estimated cost impact of each obligation/rule**. An expected and a high ('highest feasible') estimate was provided by individual responsible entities. The analysis of expected costs is provided in the sections below and the cost range (i.e., the range between the expected and high-cost estimate) is provided in Appendices S – CC. **Rough order of magnitude cost estimates** were requested from responsible entities. This reflects the inherent uncertainty of entities' cost impacts of option 2 prior to the rules being switched on. **Only the marginal impact on staff effort and/or capital/operating costs** as a result of the proposed RMP framework were included. Staff effort or costs that are already incurred or planned to be incurred were excluded from estimates. **Only costs attributable to the specified critical infrastructure asset** were included in order to avoid double-counting the cost of compliance with obligations/rules relating to other assets. Cost estimates were provided in constant ('today') dollars. The cost estimates were not escalated or indexed. Costing assumptions For the purposes of calculating a total 10-year cost of compliance with the RMP framework, **ongoing costs were assumed to commence in the year after the required implementation** (for example, for a rule requiring implementation within 2 years, the ongoing costs associated with the rule were assumed to start in year 3 of the 10-year period). The **standard unit labour price is $79.63** per hour (as advised by the Office of Best Practice Regulation); and AusCheck background checks will cost $92.50 per checked person (applicable to

Step	Description
	Personnel Hazards only). Validate costing approach with Industry The proposed costing methodology and costing template was validated with Industry.
2 Collect costing inputs to inform estimated cost of compliance for entities.	Costing templates sent to industry All responsible entities were asked to estimate costs of compliance with the RMP framework for their entity, in line with the basis for estimations and assumptions outlined in Step 1. Costings templates completed by industry 90 costing templates were received from industry across all critical infrastructure assets. These are broken down by relevant critical infrastructure asset below in section 4.1.1.
3 Calculate estimated cost of compliance for responsible entities who submitted a costing.	Calculation of estimated costs for individual entities Submissions from responsible entities were analysed to determine the estimated cost of compliance for individual entities. The one-off and ongoing cost of compliance for each entity was calculated using the following formulas: • **Total one-off cost of compliance per entity** = total one-off labour cost + one-off marginal capital costs + one-off marginal operating costs • **Total ongoing cost of compliance per entity** = total ongoing labour cost + ongoing marginal capital costs + ongoing marginal operating costs For both one-off and ongoing costs of compliance per entity, total labour costs were calculated using the following formula: **Total labour cost per entity** = marginal staff effort x standard unit labour price Targeted engagement with select entities Discussions were conducted with select entities who had submitted costs that varied substantially from other submissions. These discussions allowed for a deeper understanding of underlying factors driving cost to be developed, helped ensure the data submitted was accurate and that use of that data in the extrapolation activity (to calculate the total compliance costs for the critical infrastructure asset) was appropriate.
4 Extrapolate sector wide costs of compliance	Categorisation of costing submissions For a number of sectors, entities were categorised by size as either 'large' or 'small' entities, based on their revenue. In other sectors, alternative metrics were used. The categorisation of each critical infrastructure asset is discussed in appendices S – CC. Estimation of costs for entities that did not provide a cost submission As not every entity submitted costs of compliance, extrapolation was used to determine the overall costs for each critical infrastructure asset. The cost of compliance for entities that did not submit cost information was estimated by applying the average cost for entities of the same size and of the same critical infrastructure asset. Every cost submission received was included in the estimate of the total cost of compliance calculation. However, the average rate applied as part of the extrapolation exercise did not include the costs of entities who were managing businesses not representative of the broader critical infrastructure asset. Inclusion in the average rate applied as part of the extrapolation was determined based on discussions with those entities and/or the details of the cost assumptions provided in individual submissions.

Step	Description
	Estimation of total costs for all critical infrastructure assets The one-off and ongoing cost of compliance for each critical infrastructure asset was then calculated by adding up the individual estimates for relevant entities and adding the extrapolated cost for entities that did not make a cost submission. The total one-off and ongoing estimated cost of compliance for all critical infrastructure assets was calculated by adding up the estimates for each critical infrastructure asset. Review of cost estimates An analysis of the average cost per obligation/rule was conducted (expressed as cost per entity, cost per rule, cost per rule per dollar of revenue, etc.) to test the reasonableness of each element of the estimate. The difference between the expected and the high estimate was reviewed to understand the confidence level of submitting entities regarding the impact of each obligation/rule.
5 Estimate benefits	Approach to determining benefits Benefits of the proposed RMP framework will be accrued on a whole-of-economy level, rather than to specific organisations or individuals. Consequently, benefits were determined by quantifying the **whole-of-economy impact of actual incidents** that affected critical infrastructure assets within Australia. Benefits were calculated on the basis of **avoiding the costs of this scenario** as a consequence of the proposed RMP framework. In addition to quantified benefits, qualitative benefits were also documented and evaluated. Selection of indicative benefits scenario A different baseline benefits scenario was selected for each relevant critical infrastructure asset. The use of an actual event as the baseline risk point of comparison is important because it ensures the benefits analysis is grounded in reality. The scale of the event is not theoretical and there is sufficient information about the event to support benefits modelling. The baseline scenario used for each relevant critical infrastructure asset is discussed below in section 4.2.
6 Conduct net benefit analysis	Approach to determining net benefit: Breakeven analysis A breakeven analysis was used to determine the net benefit of option 2. The breakeven analysis examined the number of incidents that must be avoided (i.e. the benefit) each year in order for the annual costs of the regulation to be met. While this RIS sought to leverage real life examples of the potential disruptions caused by the realisation of all-hazard events, this does not mean that equivalent events must occur for the costs and benefits outlined in this RIS to break even. For example, while the critical electricity assets benefits model used the South Australian blackout as a baseline scenario, an accumulation of many, smaller disruptions would also deliver the same benefits against the proposed reforms, as discussed in section 4.2.1 below. Where real-world case studies have not been able to be sourced, alternative baseline costs have been used. These are explained further in relevant sections. Rationale for a breakeven analysis The total benefits of the RMP framework consist of the avoided or mitigated costs of future all-hazard incidents. However, the total annual benefit cannot be reliably estimated because there is no data on the frequency and size of avoided incidents. Any estimate of total benefits would be highly uncertain and reliant on assumptions. The use of a breakeven analysis avoids the need for this information, and instead uses an assessment of the reasonableness of the number of avoided incidents required for option 2 to equal or exceed the costs of the option.

Step	Description
	Breakeven analysis calculation The breakeven analysis was calculated by determining the number of severe, moderate, and low scenarios needed to be avoided each year to equal the annual cost of the regulation. The following formula was used to determine the breakeven point (severe scenario used as an example): *Number of severe scenarios required to be avoided per year for net benefit to occur = (total cost to the economy of severe scenario) / (annualised cost of regulation)* Analysis Following the calculation of the breakeven point, the results were assessed to determine the feasibility that the breakeven point would be achieved, in that the benefits of the proposed RMP framework would meet or exceed the costs.

The steps outlined above align with the Regulatory Burden Measure Framework, which directs that only particular costs associated with the introduction of the RMP framework are categorised as 'regulatory', and therefore considered when assessing likely net benefits. These costs include administrative compliance costs (associated with ensuring compliance with the proposed regulation) and substantive compliance costs (for example, the recruitment and training of new employees to meet regulatory requirements).[39]

For the purposes of this RIS, costs associated with delay (for example, expenses and loss of income incurred by a regulated entity as a result of an application delay or an approval delay) were not considered.[40] The proposed RMP framework is to be applied to existing businesses and does not include a process which may delay the operations of the regulated entities.

4.1.1. Costing submissions

There was a total of 90 costing submissions provided by responsible entities for critical infrastructure assets. See Table 7 below for a breakdown by asset class of these costing submissions, and estimated market share (where able to be calculated) by critical infrastructure asset.

Table 7 *Critical infrastructure assets cost impact submissions, number, and market share*

Critical infrastructure asset	Number of submissions	Market share (%)
Critical electricity assets	27	48.7
Critical gas assets	12	20.0
Critical water assets	7	33.3
Critical data processing or storage assets	6	N/A
Critical broadcasting assets	2	100.0
Critical financial market infrastructure assets (payment systems)	2	28.7

[39] Department of Prime Minister and Cabinet, 2020

[40] Department of Prime Minister and Cabinet, 2020

Critical domain name systems	1	100.0
Critical liquid fuels assets	0[41]	0
Critical hospitals	23	90.0
Critical energy market operator assets	2	N/A
Critical freight infrastructure *and* critical freight services assets[42]	5	32.2
Critical food and grocery assets	3	90.5
Total	**90**	

With the exception of critical hospital assets, the market share percentage of responsible entities who made a submission was calculated for all assets using entity and sector data sourced from IBISWorld. The market share percentage was determined using entity revenue as a percentage of total critical infrastructure asset revenue.

The 'market share' percentage of critical hospital entities was calculated using the ICU bed capacity of those entities which provided a cost submission. Total ICU bed capacity was then used to extrapolate the compliance costs for all critical hospital assets in Australia.

Market share was not calculated for critical data storage or processing assets due to insufficient data on the total revenue in the critical data storage or processing asset market. Although the revenue of submissions was able to be calculated, as there was no verifiable data on the total revenue, the market share of submissions could not be calculated. Market share was also not calculated for critical energy market operator assets, as revenue was not able to be divided between responsible entities in the asset class.

4.2. Likely net benefit of each option

The following sections detail the estimated costs and benefits, and overall likely net benefit, associated with each option considered by this RIS. For options 1 and 3, the discussion is largely focused on qualitative costs and benefits, while option 2 is evaluated through a breakeven analysis, as discussed above.

As part of the net benefit assessment, real world scenarios and associated costs are utilised to model the cost of avoided future incidents (by critical infrastructure asset). Table 8 below provides the total cost to the economy (direct and indirect costs) of each baseline scenario utilised, and the impact size at which the baseline scenario was defined (specifically as a low, moderate, or severe incident). For some asset classes, multiple baseline scenarios were used. Further detail can be found in appendices S – CC. The method is discussed further in section 4.2.2.

Table 8 *Critical infrastructure assets baseline scenario total cost to the economy*

Critical infrastructure asset	Baseline scenario total cost ($ million)	Impact size of baseline scenario
Critical electricity assets	850.0	Moderate
Critical gas assets	1,913.0	Severe

[41] No responsible entity for critical liquid fuel assets submitted an estimated cost of compliance. To estimate the cost of compliance for the liquid fuels sector, the average cost of compliance of similar sized entities in the gas sector was used as the base cost for liquid fuel entities. Critical gas asset entity submissions were used as the baseline as critical gas asset entities operate comparable businesses

[42] The costing process for these two critical infrastructure assets was consolidated.

Critical infrastructure asset	Baseline scenario total cost ($ million)	Impact size of baseline scenario
Critical water assets	4,099.0	Severe
	126.8	Moderate
	1.2	Low
Critical data processing or storage assets	98.0	Moderate
	4.6	Low
Critical broadcasting assets and critical domain name systems[43]	3.8	Moderate
Critical financial market infrastructure assets (payment systems)	13.5	Moderate
Critical liquid fuels assets	1,931.0	Severe
	14.5	Low
Critical hospitals	229.8	Severe
Critical energy market operator assets	850.0	Moderate
Critical freight infrastructure and critical freight services assets[44]	724.1	Severe
	18.1	Low
Critical food and grocery assets	48.0	Moderate

4.2.1. Likely net benefit: Option 1

This section summarises the qualitative costs and benefits associated with option 1, before assessing the likely net benefit derived from option 1.

Costs of option 1

Under option 1, the status quo would be maintained, and no additional regulatory measures would be imposed on critical infrastructure assets. The status quo provides a baseline for benefits and costs if nothing is done and can be used as a comparator with option 2 and 3. The most significant cost associated with option 1 is industry's ongoing exposure to the risks associated with all hazard threats, which are rapidly outpacing the current regulatory environment.

For the purposes of modelling the potential costs associated with the realisation of all-hazard threats for critical infrastructure assets, the incidents described in section 4.2.2 and costed in Table 9 were used for each relevant critical infrastructure asset. For the purposes of modelling the potential costs, a single example is sufficient to demonstrate the potential disruptions arising from the realisation of all-hazard threats. The chosen examples are founded in real events, with sufficient reliable information available to support the economic modelling undertaken.

While this RIS uses these baseline scenario examples for each asset, it does not mean that a single event equivalent to each respective baseline scenario is needed for costs and benefits to break even. The chosen examples are intended to be demonstrative of the potential costs of a disruption to critical infrastructure, rather than demonstrative of the specific events which may lead to disruption. The examples used are typically specific types of hazard events, for every relevant

[43] The net benefit assessment for these two assets was consolidated.

[44] The net benefit assessment for these two assets was consolidated.

critical infrastructure asset the disruption could also be as a result of one or more other hazards. It may be the case that a series of smaller, less significant disruptions occur over the course of a year, and accumulate to deliver a resulting disruption of a magnitude similar to that resulting from more severe scenarios. Equally, a more significant disruption could occur, but less frequently, for the same cost to be incurred.

A baseline scenario is used with costs scaled up or down for the other incident sizes. For example, the baseline scenario for electricity is used as the 'moderate' scenario, with costs scaled up for the electricity severe scenario and down for the low scenario. The total cost of an incident consists of direct and indirect costs. The direct costs refer to the financial costs directly incurred as a result of an incident, while indirect costs refer to flow-on costs to the economy due to supply chain linkages and other feedback responses by all economic agents (e.g., households, businesses). Specifically, the indirect costs include impacts to consumers as a result of the costs of an incident being passed on through future price increases.

Table 9 below indicates the potential costs associated with the realisation of all-hazard threats for critical infrastructure assets.

Table 9 *Total cost to the economy (direct and indirect costs) of the incident, by critical infrastructure asset*

Critical infrastructure asset	Scenario 1 (Severe, $ million)	Scenario 2 (Moderate, $ million)	Scenario 3 (Low, $ million)
Critical electricity assets	1,280.0	850.0	490.0
Critical gas assets	1,913.0	1,001.0	513.0
Critical water assets	4,099.0	126.8	1.2
Critical data processing or storage assets	196.0	98.0	4.6
Critical broadcasting assets *and* critical domain name systems[45]	7.7	3.8	1.9
Critical financial market infrastructure assets (payment systems)	27.1	13.5	6.8
Critical liquid fuels assets	1,913.0	1,001.0	14.5
Critical hospitals	229.8	114.9	23.0
Critical energy market operator assets	1,280.0	850.0	490.0
Critical freight infrastructure and critical freight services assets[46]	724.1	362.1	18.1
Critical food and grocery assets	72.0	48.0	24.3

These costs are broken down further for each critical infrastructure asset in appendices S – CC.

The costs outlined in the table above are discussed in greater detail in the section 4.2.2 below. Without adequate protections, industry and the Australian economy as a whole may incur costs in line with those described above, dependent on the severity and frequency of the disruption.

Benefits of option 1

Under option 1, industry 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.

Assessment of likely net benefit

The costs and benefits set out above demonstrate that option 1 is not capable of achieving a coordinated uplift in all-hazards risk management across critical infrastructure assets, as this option involves no change to the current regulatory environment. While, under the status quo,

[45] The net benefit assessment for these two critical infrastructure assets was consolidated.

[46] The net benefit assessment for these two critical infrastructure assets was consolidated.

industry will face no increase in regulatory costs, stakeholders will suffer the forgone benefit of clear direction and consistent standards set by Government. Without the benefit of an uplift in the security and resilience of all critical infrastructure assets, critical infrastructure assets are left more vulnerable to the realisation of all-hazard incidents. As a result, industry may bear the associated cascading consequences and financial costs outlined above.

4.2.2. Likely net benefit: Option 2

The following section details the costs and benefits associated with option 2 (mandatory RMP framework), before assessing the overall likely net benefit presented by this option.

Costs of option 2

There are multiple factors affecting the regulatory burden for each entity, including their existing risk management practices and capabilities, the nature of the critical infrastructure assets they operate, and the size of their operations. In collecting cost information from entities across critical infrastructure assets, this variance in cost impact has been captured and reflected in the estimates of total cost across critical infrastructure assets included in this RIS.

The expected costs associated with option 2 are estimated as follows:

- A one-off aggregated cost of $1,601.0 million, across critical infrastructure assets nationally, to achieve compliance with the RMP obligations and RMP rules; and
- An ongoing aggregated cost of $1,076.3 million per year, across critical infrastructure assets nationally, to maintain compliance.

The cost of regulation will be borne by entities responsible for critical infrastructure assets who meet the relevant thresholds. Community organisations and individuals will not be directly affected but there will likely be indirect costs passed onto consumers. For the purposes of this RIS, the cost of regulation in Table 10 will only include the initial costs associated with regulation.[47] The indirect cost to consumers and communities has been addressed in the economic analysis detailed in the net benefit section below. This considers the indirect costs and benefits to the wider economy as a result of the proposed RMP framework.

***Table 10** Regulatory cost estimate*

Cost Type	Costs ($ million)			
	Business	Community	Individuals	Total cost
One-off	1,601.0	Nil	Nil	1,601.0
Ongoing (per year)	1,076.3	Nil	Nil	1,076.3

Note: There will be no direct costs to individuals and communities although price rises may reflect the increased cost of operations as a result of the proposed RMP framework.

The total regulatory cost estimate was based on submissions from industry which are summarised in Table 10. The average regulatory cost estimate per submission for each critical infrastructure asset type is provided in

Table **11**.

[47] Department of Prime Minister and Cabinet, 2020

Table 11 *Average regulatory cost per critical infrastructure asset submission*

Critical infrastructure asset	Costs ($ million)	
	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
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	**7.9**	**3.6**

Table 12 *Regulatory cost estimate per critical infrastructure asset*

Critical infrastructure asset	Costs ($ million)				
	Total one-off costs **(a)**	Total annual ongoing costs	Total ongoing cost over a ten-year period[48] **(b)**	Total costs over a ten-year period **(c) = (a)+(b)**	Total average annual cost over a ten-year period **(c) divided by 10**
Critical electricity assets	463.3	228.0	2,115.6	2,578.9	257.9
Critical gas assets	321.1	94.0	831.8	1,152.9	115.3
Critical water assets	157.5	91.1	849.4	1,006.9	100.7
Critical data processing or storage assets	116.6	296.9	2,779.0	2,895.7	289.6
Critical broadcasting and domain name system assets[49]	2.1	1.5	14.0	16.2	1.6
Critical financial market infrastructure assets (payment systems)	0.6	5.7	53.1	53.7	5.4
Critical liquid fuels assets	35.8	10.5	95.7	131.5	13.2
Critical hospitals	342.6	265.1	2,394.7	2,737.3	273.7
Critical energy market operator assets	88.3	26.9	241.4	329.7	33.0
Critical freight infrastructure *and* critical freight services assets[50]	60.9	50.0	467.0	527.8	52.8
Critical food and grocery assets	12.2	6.6	60.7	72.9	7.3
Total costs	**1,601.0**	**1,076.3**	**9,901.8**	**11,503.6**	**1,150.4**

The regulatory cost estimate is broken down by relevant critical infrastructure asset in appendices S – CC.

[48] For the purposes of calculating a total 10-year cost of compliance with the risk management program framework, ongoing costs were assumed to commence in the year after the required implementation date (for example, for a rule requiring implementation within 2 years, the ongoing costs associated with the rule were assumed to start in year 3 of the 10 year period).

[49] The net benefit assessment for these two Critical Infrastructure assets was consolidated.

[50] The net benefit assessment for these two Critical Infrastructure assets was consolidated.

Benefits of option 2

Reliable critical infrastructure is central to Australia's prosperity. Further, disruption to supply, compromise of operation, or other impacts can have a significant cost to the economy. The RMP framework aims to reduce the frequency and impact of any disruption to availability, integrity, reliability, or confidentiality of critical infrastructure, and so its primary benefit is to avoid the incidents that may otherwise disrupt operation and lead to economic loss.

Computable General Equilibrium (CGE) modelling was used to illustrate how costly disruption to critical infrastructure assets could potentially be by examining a hypothetical 'shock' (the nature of which varied between relevant critical infrastructure assets) and an associated increase in input costs (i.e., an increase in the cost of the service). The advantage of using a CGE approach is that both the direct and indirect (i.e. flow-on) economic impacts of an event can be quantified.

CGE modelling approach

To analyse the direct and indirect economic contributions of the baseline scenario events due to disruptions to critical infrastructure on the Australian economy, a CGE approach was used to model 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.

Scenarios

The CGE modelling provided estimates regarding how sensitive the Australian economy is to a shock to each of the relevant critical infrastructure assets. The method of analysis remained consistent across all relevant critical infrastructure assets, with any minor adjustments explained in the relevant appendix. 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.

Case studies

Case studies provide a basis for modelling hypothetical, but comparable, events, in an economy-wide model and contextualising the results of that modelling. The case studies have been chosen to provide insights into the economy-wide costs to households and businesses of large-scale and severe disruption events. The case studies are summarised in the Table 13 below and described in detail in appendices S – CC for each relevant critical infrastructure asset:

Table 13 *Baseline scenario case study summary*

Critical infrastructure asset	Baseline scenario
Critical electricity assets	South Australian blackout (2016)
Critical gas assets	Varanus Island disruption (2008)
Critical water assets	Queensland floods (2011) Sydney water crisis (1998) UK water supplier scam (2017)
Critical data processing or storage assets	Kaseya outage (2021) Former employee targets Cisco Systems (2018)
Critical broadcasting assets *and* critical domain name systems[51]	South Coast transmitter burnout (2020)
Critical financial market infrastructure assets (payment systems)	NAB service disruption (2018)
Critical liquid fuels assets	Varanus Island disruption (2008) Colonial Pipeline cyber-attack (2021)
Critical hospitals	NHS WannaCry ransomware attack (2017)
Critical energy market operator assets	South Australian blackout (2016)
Critical freight infrastructure *and* critical freight services assets[51]	TNT Express cyber-attack (2017) ForwardAir ransomware attack (2020)
Critical food and grocery assets	Coop Supermarket closures (2021) JBS meat processing ransomware attack (2021)

[51] The costing and benefit analysis process for these two critical infrastructure assets was consolidated.

An example framework for considering the potential impacts of a disruption event following (or due to) failure of critical infrastructure is provided in Table 144 below:

Table 14 *Example framework for scenario development and sensitivity analysis*

	Severe scenario	Moderate scenario	Low scenario
Intensity of event	Increased percentage of baseline scenario costs	Baseline event	Lower percentage of baseline scenario costs

Note: in some cases, the baseline scenario is used as the 'severe' or 'low' scenario, and in some cases, there are multiple baseline scenarios used for a relevant critical infrastructure asset.

The rationale for a more severe scenario than experienced in the identified baseline scenario reflects the complexity of the scenarios that could occur. As noted above, the economic impact of an incident will vary due to a range of factors including the location of a disruption, the month and time of day at which the disruption occurs, the day of the week on which the disruption takes place, and the duration of disruption. Accounting for an incident that has a greater economic impact than the baseline scenario is necessary to reflect the possibility that a disruption of the same scale could impact areas where there would be greater economic impact than in the baseline scenario. While an incident with a much greater impact than the severe scenario could also be conceivable, the defined scenarios and subsequent benefits analysis has taken a deliberately conservative approach to ensure the severe scenario remains demonstrably plausible.

A summary of the total avoided cost to the economy of the incident for each relevant critical infrastructure asset is provided in Table 15. Direct avoided costs refer to the financial costs directly incurred as a result of an incident, while indirect costs refer to flow-on costs to the economy due to supply chain linkages and other feedback responses by all economic agents (e.g. households, businesses). A break-even analysis of these benefits compared to the total estimated cost of the RMP framework is also included in the table. This break-even analysis is expressed as the number of incidents that would need to be avoided in order for the benefits (that is, the avoided costs) of the RMP framework to equal the costs of implementation and compliance.

Table 15 *Summary of benefits scenarios*

Critical infrastructure asset		Scenario 1 (Severe), $ million	Scenario 2 (Moderate), $ million	Scenario 3 (Low), $ million
Critical electricity assets	Total avoided cost to the economy of the incident	1,280.0	850.0	490.0
	Approximate number of avoided incidents per annum required for a net benefit	0.5	0.7	1.2
Critical gas assets	Total avoided cost to the economy of the incident	1,913.0	1,001.0	513.0
	Approximate number of avoided incidents per annum required for a net benefit	0.1	0.2	0.3
Critical water assets	Total avoided cost to the economy of the incident	4,099.0	126.8	1.2
	Approximate number of avoided incidents per annum required for a net benefit	Less than 0.1	1.8	197.5
Critical data processing or	Total avoided cost to the economy of the incident	196.0	98.0	4.6

Critical infrastructure asset		Scenario 1 (Severe), $ million	Scenario 2 (Moderate), $ million	Scenario 3 (Low), $ million
storage assets	Approximate number of avoided incidents per annum required for a net benefit	3.8	7.5	160.1
Critical broadcasting assets and critical domain name systems	Total avoided cost to the economy of the incident	7.7	3.8	1.9
	Approximate number of avoided incidents per annum required for a net benefit	0.9	1.8	3.6
Critical financial market infrastructure assets (payment systems)	Total avoided cost to the economy of the incident	27.1	13.5	6.8
	Approximate number of avoided incidents per annum required for a net benefit	0.4	0.9	1.7
Critical liquid fuels assets	Total avoided cost to the economy of the incident	1,913.0	1,001.0	14.5
	Approximate number of avoided incidents per annum required for a net benefit	Less than 0.1	Less than 0.1	1.1
Critical hospitals	Total avoided cost to the economy of the incident	229.8	114.9	23.0
	Approximate number of avoided incidents per annum required for a net benefit	4.1	8.1	40.7
Critical energy market operator assets	Total avoided cost to the economy of the incident	1,280.0	850.0	490.0
	Approximate number of avoided incidents per annum required for a net benefit	Less than 0.1	Less than 0.1	0.1
Critical freight infrastructure and freight services assets	Total avoided cost to the economy of the incident	724.1	362.0	18.1
	Approximate number of avoided incidents per annum required for a net benefit	0.4	0.8	15.6
Critical food and grocery assets	Total avoided cost to the economy of the incident	72.0	48.0	24.3
	Approximate number of avoided incidents per annum required for a net benefit	Less than 0.2	Less than 0.3	0.5

Consideration of the feasibility of achieving a breakeven point for each critical infrastructure asset is not only dependent on the number of incidents required to breakeven, but also on the likelihood of an incident occurring as well as the scale of the sector. For example, for critical data processing and storage assets, the nature of the modelled the 'low' impact incident affected a single organisation and its customers. The quantum of responsible entities in that asset class means that the number of incidents avoided required to yield a net benefit is spread across a larger number of

entities than other asset classes (the Department estimates the number of responsible entities for critical data storage or processing assets exceeds 300). Therefore, although there are a significant number of incidents required for a net benefit in the 'low' impact scenario, the evidence indicates that a positive net benefit is achievable and likely given that the nature of the incidents experiences frequently involves a large number of entities. The breakdown of direct and indirect costs (which make up the total avoided cost to the economy of the incident) for each relevant critical infrastructure asset is contained in appendices S – CC.

For critical water assets and critical hospitals, the economic benefit of avoiding incidents should also be considered alongside the avoided cost to human life. The estimated value of a statistical life (the value society places on reducing the risk of dying) is $5.1 million, and the value of a statistical life year (the value society places on a year of life) is $0.2 million.[52] As both critical water assets and critical hospitals are critical to human life, any avoidance of a disruption to critical hospitals that could have otherwise increased the likelihood of disease, illness or death will have a benefit beyond that of the avoided cost to the economy able to be modelled.

It is important to note that the economic analysis of the above scenarios does not incorporate all direct avoided costs incurred by all future incidents. The avoided costs included are only those which were directly and immediately incurred as a result of the identified baseline scenario for that asset. In the broader context of a potential future disruption, in addition to the above estimate of benefits could be the avoided costs of recovery (repair costs, costs of resulting mitigations) from high value, specific circumstances which were not experienced as part of the identified baseline case study.

Further, the increasing frequency of incidents as described in section 1.1 makes the proposed RMP framework more certain over time to exceed the anticipated costs. The examples referred to in that section demonstrate the increasing need for adequate protections against the security and resilience of critical infrastructure assets, and the increased likelihood that the benefits of the draft RMP framework will exceed the costs outlined in this section.

Assessment of likely net benefit

The likely benefits of option 2 will be at least (and are expected to be more than) the costs of the regulation. This is primarily because, as described above and throughout this RIS, the frequency and severity of all-hazard risks for critical infrastructure assets are growing. While some events of the magnitude described in this RIS 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, as described above, makes the proposed RMP framework more likely to exceed the anticipated costs over time.

Further, through pursuit of option 2, the identification, mitigation, and remediation of such hazards, should they occur, will be improved through:

- Lowering the material risk of hazards, and subsequent impacts of those hazards, as they manifest for critical infrastructure assets;
- Ensuring that adoption of the RMP framework for critical infrastructure assets is reasonable and proportionate to the purpose of the program;
- Avoiding regulatory duplication and facilitating a coordinated uplift in responsible entities' compliance with relevant standards; and
- Improving Government's visibility over the security and resilience of critical infrastructure assets.

[52] Abelson 2007

Overall these factors, and the specific costs and benefits described above, mean the likely net benefit associated with option 2 is high.

4.2.3. Likely net benefit: Option 3

The following section details the costs and benefits associated with option 3 (voluntary RMP and guidance), before assessing the overall likely net benefit presented by this option.

Costs

Responsible entities who choose to voluntarily implement parts of the RMP or associated guidance will incur costs of anywhere between option 1 (status quo) and option 2 (regulation), depending on the degree to which they decide to implement these parts.

The maximum, average expected cost of compliance for an entity who chooses to voluntarily meet the guidance is estimated as $7.9 million in one-off costs and $3.6 million per year in ongoing costs, noting that there is a wide range provided in submissions from industry. A further breakdown of the costs is provided in appendices S – CC for each relevant critical infrastructure asset.

For responsible entities who choose not to voluntarily implement the RMP framework, the costs incurred will be the same as those costs associated with option 1 above. 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 RIS. These risks are rapidly outpacing the current regulatory environment. Table 16 below indicates the potential costs associated with the realisation of all-hazard threats for critical infrastructure assets.

***Table 16** Total potential cost to the economy (direct and indirect costs) of the incidents, by critical infrastructure asset*

Critical infrastructure asset	Scenario 1 (Severe, $ million)	Scenario 2 (Moderate, $ million)	Scenario 3 (Low, $ million)
Critical electricity assets	1,280.0	850.0	490.0
Critical gas assets	1,913.0	1,001.0	513.0
Critical water assets	4,099.0	126.8	1.2
Critical data processing or storage assets	196.0	98.0	4.6
Critical broadcasting assets and critical domain name systems	7.7	3.8	1.9
Critical financial market infrastructure assets (payment systems)	27.1	13.5	6.8
Critical liquid fuels assets	1,913.0	1,001.0	14.5
Critical hospitals	229.8	114.9	23.0
Critical energy market operator assets	1,280.0	850.0	490.0
Critical freight infrastructure *and* critical freight services assets[53]	724.1	362.0	18.1
Critical food and grocery assets	72.0	48.0	24.3

Note: for a description of the baseline scenarios used for each critical infrastructure asset, see appendices S – CC.

[53] The net benefit assessment for these two critical infrastructure assets was consolidated.

Without adequate protections, industry and the Australian economy as a whole may incur costs in line with those described above, dependent on the severity and frequency of the disruption.

In the current regulatory environment, Government has limited visibility of current risk management practices to support industry in the identification and mitigation of potential all-hazard threats. Further, should such a threat be realised, Government has little opportunity to support industry in managing remediation efforts. This limited visibility and limited ability to ensure risks are appropriately managed compounds the costs described above.

Benefits

Under option 3, industry will experience some of the benefits associated with option 2 above, and the qualitative benefits discussed in this section, to the extent that industry chooses to comply with the voluntary RMP framework. Consequently, there may be some degree of uplift in all hazards risk management across some critical infrastructure assets, for those who choose to implement aspects of the RMP framework. Further, the voluntary approach offers some flexibility for industry in choosing its approach to risk management. This may assist in managing deviations between responsible entities and Government's risk appetites. However, as the benefits of option 2 predominantly relate to benefits resulting from a sector-wide uplift, the benefits accruing to individual organisations that comply with the voluntary RMP framework will be reduced substantially.

Assessment of likely net benefit

The costs and benefits set out above demonstrate that responsible entities who choose not to voluntarily implement the RMP framework will not contribute to achieving a coordinated uplift in all hazards risk management across critical infrastructure assets.

In considering the costs and benefits described above, the likely net benefit of option 3 is likely higher than pursuing option 1, but lower than the likely net benefit offered by option 2. This is because the voluntary format of option 3 means that it is unlikely to achieve an uplift in all hazards risk management across critical infrastructure assets. Despite the benefits received by those responsible entities who choose to voluntarily implement the RMP framework, it is unlikely that compliance will be achieved across sector critical infrastructure assets. In addition to leaving critical infrastructure assets vulnerable to the consequences of all-hazard threats, option 3 therefore presents less economy-wide benefit.

5. Consultation and feedback

5. Consultation and feedback

This section provides an overview of the Department's consultation process for RMP obligations, including an explanation of the purpose and objectives of the consultation, key feedback themes that emerged and how these have been, and are being, considered in policy design.

5.1. Purpose and objectives of consultation

Continuous and broad-based consultation is an essential component of the Department's consultation process for RMP rules. Effective consultation ensures that all enacted reforms are implemented in a manner that secures desired outcomes, while minimising any unnecessary or disproportionate regulatory burden or duplication on the affected sector.[54]

The sector-specific elements of the consultation process reflect the Department's view that each industry manages risk in a unique way, and that industry stakeholders themselves are best-placed to identify, evaluate, and mitigate the risks which manifest in their particular sector. The Department acknowledges and seeks to avoid prescriptive RMP obligations, which have the potential to disrupt industry's ability to respond to risks in a nuanced manner. Effective consultation was critical for the Department; it validated that a principles-based approach was preferred by industry, and which will allow organisations to continue managing their risks in a manner most appropriate for their operating context.

Avoiding regulatory duplication is an additional goal for the Department in delivering the SLACIP Act's RMP obligations. In developing new regulation, including the proposed RMP rules, the SLACIP Act requires the Minister of Home Affairs to consider any existing regulatory systems by the federal government, a State or a Territory Government that imposes obligations on responsible entities. Government's position remains that where a critical infrastructure sector or asset is already subject to a regulatory regime which comprehensively addresses (and through which entities achieve) the same outcomes sought by the implementation of RMP obligations, these will not be duplicated.[55]

[54] Department of Home Affairs, 2021, p. 2

[55] Department of Home Affairs, 2021, p. 2

Table 17 below contains an overview of the stakeholder organisations consulted during the consultation process across all critical infrastructure sectors:

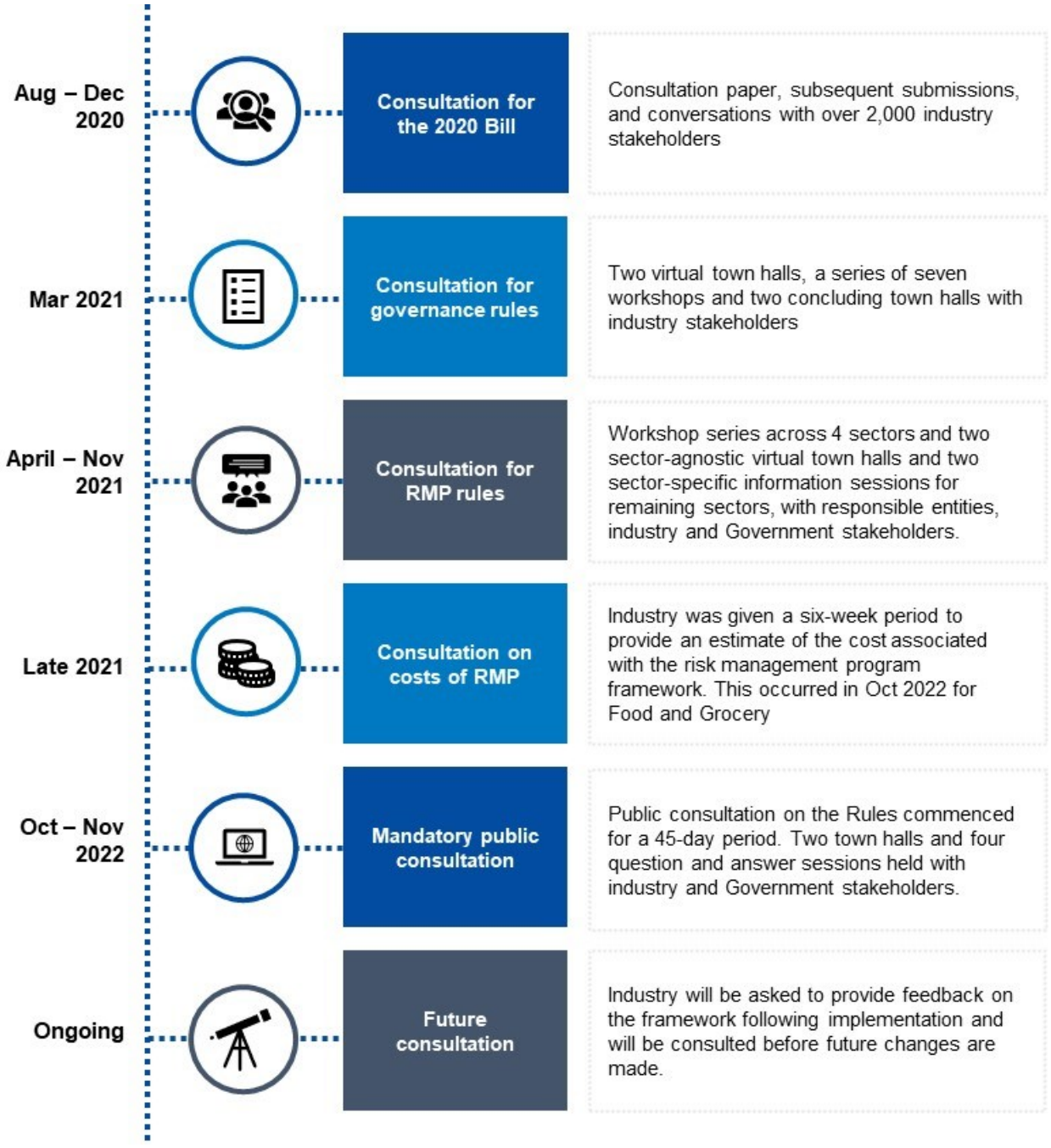
Table 17 *Overview of responsible entities consulted*

Asset Class	Number of Stakeholders Consulted (approx.)
Electricity	67
Gas	10
Water	28
Data	52
Broadcasting	2 (all entities captured)
Financial Market Infrastructure (Payment Systems)	4 (all entities captured)
Domain Name Systems	1 (all entities captured)
Liquid Fuels	7
Critical Hospitals	85
Energy Market Operator	4 (all entities captured)
Freight Infrastructure / Freight Services	10
Food and grocery	4 (all entities captured)
Total	**274**

5.2. Consultation process

This section provides an overview of previous consultation, including brief discussion of consultation for the 2020 SLACI Bill, the (then) governance rules (now general rules) and the RMP rules, and a roadmap for future consultation, as summarised by Figure 3 below.

Figure 3: *Consultation timeline*



5.2.1. Previous consultation

Consultation: SLACI

Consultation on the regulatory measures within this RIS builds upon and leverages previous and comprehensive engagement conducted in relation to the 2020 SLACI Bill, the 2021 SLACI Act and the SLACIP Act. Extensive consultation preceded the introduction of the SLACI Bill, as captured in the 2020 RIS. Consultation through a paper titled 'Protecting Critical Infrastructure and Systems of

National Significance', which proposed regulatory and non-regulatory proposals to protect Australia's critical infrastructure from all-hazard threats, occurred in August and September 2020. The Department met with over 2,000 industry stakeholders from over 54 entities and received 194 submissions in response to the consultation paper, including from all states and territories, by the close of the submission period on 16 September 2020. Non-confidential submissions are available on the Home Affairs' website.

Key concerns raised, and how they were addressed in response to the consultation paper, are highlighted in Table 18 below.

Table 18 *Concerns and responses to consultation paper 'Protecting Critical Infrastructure and Systems of National Significance'*

Stakeholder Concern	Action by Department
Lack of clarity about what assets were to be critical infrastructure assets.	The Department sought to gain a more detailed understanding of each sector, permitting a more nuanced approach to identifying captured assets.
The potential for duplication of existing regulatory frameworks.	'On switches' were developed for positive security obligations, ensuring such obligations were only imposed where there is no comparable, existing regulatory framework.
The potential for regulatory impost and the proportionality of requirements.	Consultation on the RMP rules was proposed, to ensure robust discussion as to the manner and form of proposed rules to ensure that rules are reasonable and proportionate.
The threshold for engaging Government assistance was too low.	The Department introduced additional safeguards, to position Government's powers to intervene as a last resort method of intervention.

Some stakeholders proposed alternative approaches to building critical infrastructure security and resilience, which the Department has not progressed. These included, for example, a vulnerability disclosure scheme; a national critical service overlay network; and the use of environmental surveillance network instrumentation to show changes to risk leading indicators in near real time.

Further, on 9 November 2020, an exposure draft of SLACI Bill was released (accompanied by an explanatory document) for public consultation. At the conclusion of consultation on 27 November 2020, discussions with 1,000 individuals occurred in response to the exposure draft, and 129 submissions were received. Non-confidential submissions are available on the Home Affairs' website.

Table 19 below outlines the key changes made in response to consultation.

Table 19 *Concerns and responses – exposure draft of the SLACI Bill*

Stakeholder concern	Action by Department
Some assets that are not critical may be captured by the Bill.	Asset definitions were refined to reflect only those assets that are truly critical. Provisions were also added that allow for the rules to provide that particular elements of the positive security obligations do not apply to an asset, even if it is classified as a critical infrastructure asset.
Consultation requirements are insufficient.	Broader and extended timeframes for consultation was embedded in the legislation including, for example: • Before making or amending the rules, the Minister must publish these on the Home Affairs website for 28 days and consider any submissions made within this period. • Before making any rules relating to the critical infrastructure RMP, the Minister must have regard to any existing regulatory system of

	the Commonwealth, a State or Territory that imposes obligations on responsible entities. • Before giving a notice to an entity under the enhanced cyber security obligations, the Secretary must consult the relevant entity, and, if there is a relevant Commonwealth regulator that has functions relating to the security of that system – the relevant Commonwealth regulator.
It is unclear how The Department will identify an entity as a system of national significance.	Greater clarity on the criteria for declaring a system as a system of national significance was included in SLACIP Act. Additions included specifying that in determining whether an asset is a system of national significance, the Minister must have regard to the consequences that would arise for the social or economic stability of Australia or its people; or the defence of Australia; or national security if a hazard were to occur that had a significant relevant impact on the asset.
Timeframes for reporting cyber security incidents as part of the notification of cyber security incidents obligation are too short.	Reporting timeframes for cyber security incidents were extended from 24 hours to 72 hours for some types of cyber security incidents.

Feedback received on the original SLACI exposure draft of the Bill remained consistent with that received on the consultation paper, with broad in-principle support for the uplift to the security and resilience of critical infrastructure and the need to enhance Government's security-focused relationship with industry. Further, information on other suggestions made by stakeholders in response to the exposure draft for SLACI Bill, and how the Government responded to these, is available in the 2020 RIS.

The SLACI Bill was then introduced to Parliament on 10 December 2020.

Consultation: General rules

Following the introduction of the SLACI Bill to Parliament, engagement with industry continued. The Department commenced its industry consultation process in March 2021, with the development of sector-agnostic general rules. Given the sector-agnostic design of the general rules, consultation did not occur on a sector-specific basis. As stated earlier, at the time of consultation, these were referred to as governance rules.

Consultation occurred in three key stages:

1. **Two virtual town halls,** held on 2 and 4 March 2021 and attended by approximately 850 participants, introduced the idea of the general rules. The town halls aimed to provide industry with a greater understanding of what they will need to consider in the development of their RMP.
2. **Through a series of seven workshops**, held over a two-week period from 8 March 2021, Government and industry worked collaboratively to agree on key areas that should be codified through rules including context identification processes, siloes, and accountability and risk methodology and reviews. Over 500 industry and government stakeholders attended the workshop series.
3. **Two concluding town halls** were conducted on 29 and 30 March 2021 to present and finalise the outcomes of the co-design process.[56]

Table 20 below details the discussion on key themes which emerged during industry co-design of general rules:

[56] Department of Home Affairs 2021, p. 2

Table 20 Key themes from general rule consultation

Rule category	Identified themes	Impact on development of rules
General rules	• Industry suggested their **current business practices broadly achieve the objectives of the proposed RMP**. Participants advised they had already implemented risk management plans either for business continuity purposes or as a requirement of existing regulation. • Industry participants expressed concern with apparent overlap of RMP requirements and existing regulation. • There was general agreement among industry that **general rules must not be overly prescriptive**. Participants advised that each industry sector manages risks in a unique way. Broadly applied prescriptive rules may disrupt industry's ability to respond to unique challenges. By following a more principles-based approach, each business could continue to manage their own risks in the way that works best for its context.	In response to feedback received during consultation for general rules, the Department committed to: • ensuring that minimising regulatory duplication remains a top priority; • striving for clarity whilst avoiding prescriptiveness where appropriate, providing industry with sufficient flexibility to recognise the unique circumstances of their business; • providing guidance material to industry to ensure smooth implementation of the requirements under the Program; and • designing rules so as not to disrupt existing good practices in mature entities, but to uplift practices within less mature entities.

As demonstrated in Table 20 above, consultation saw industry emphasise the need to leverage existing regulatory frameworks and risk management processes, in order to avoid duplication. A key mechanism for avoiding regulatory duplication is Government's ability to identify those critical infrastructure assets which are subject to existing obligations comparable to the obligations contained in the RMP and, therefore, choose not to 'switch on' the relevant RMP obligations for those assets.

5.2.2. RMP rules consultation

The Department undertook extensive consultation with industry for the design of RMP rules, with the objectives of:

- Assessing whether there are existing regulations that meet the RMP objectives, to ensure the regulatory burden is reduced where possible; and
- Ensuring there are rules in place that will drive an uplift in the security and resilience of critical infrastructure assets.[57]

Consultation with industry stakeholders occurred across the following stages:

- **A series of sector-specific workshops** across four asset classes (electricity, gas, water, and data), held from April to August 2021. These workshops provided a forum to design the RMP Rules and assisted in understanding the costs and benefits associated with implementing the risk management program framework. Workshops were designed to provide:
  - Several opportunities for discussion and feedback to gather industry perspectives;
  - Polling, in-session surveys and facilitated discussions; and

[57] Department of Home Affairs, 2021, p. 2

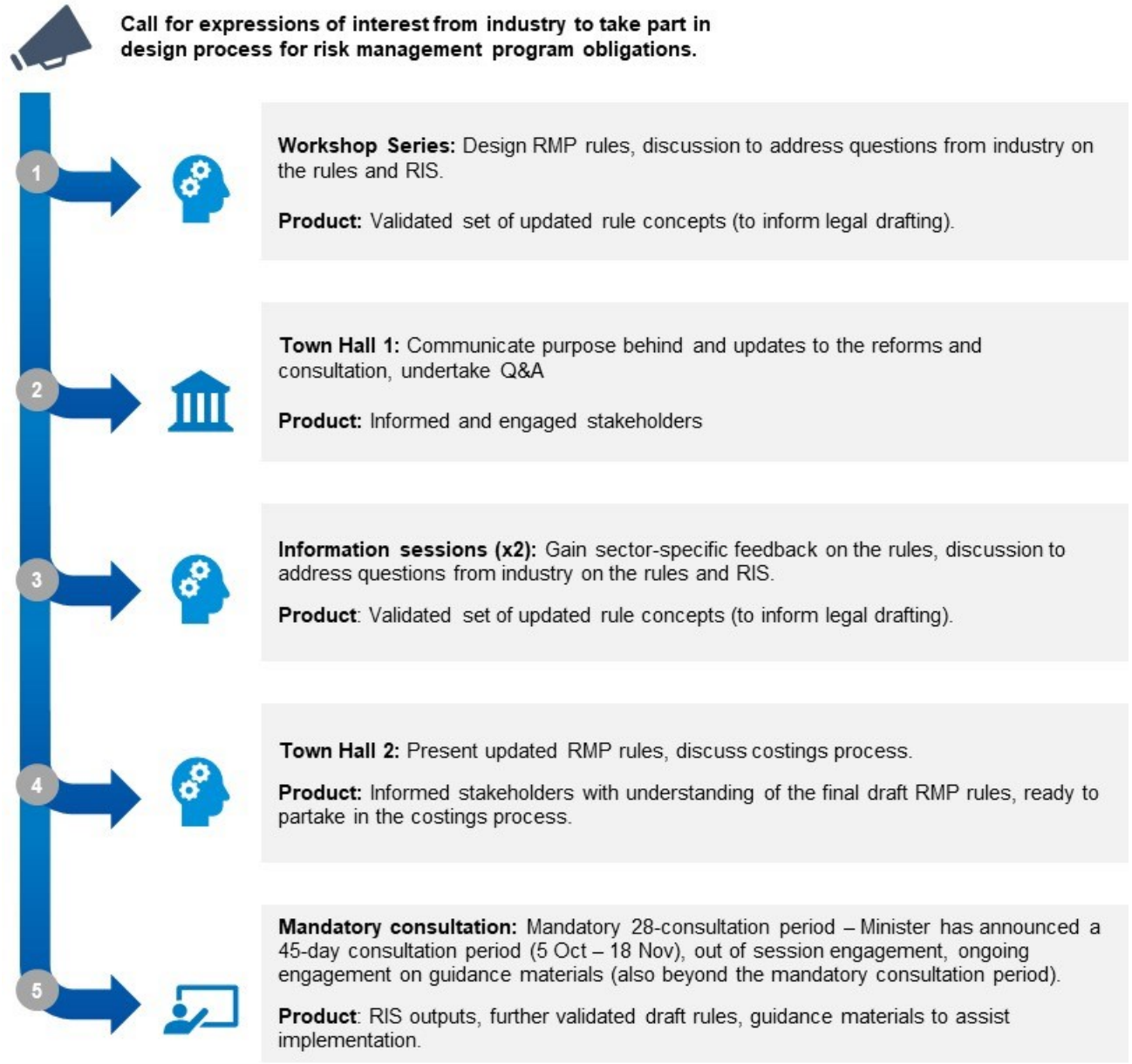
  - ‘Break out room’ discussions, to ensure comprehensive discussion occurred across all subsets of industry.
  - **Two sector-specific Information Sessions** held in October and November 2021 for each sector, across all critical infrastructure asset classes which would be subject to the RMP obligation. The purpose of the information sessions was to provide an update for industry on the move from sector-specific to sector-agnostic RMP rules, and to gain sector-specific feedback on the updated RMP rules.

- **Two industry-agnostic Town Halls** held in October and November 2021. The purpose of the first Town Hall was to provide an update for industry on the move from sector-specific to sector-agnostic RMP Rules. The purpose of the second Town Hall was to present the updated RMP rules, and provide information on the further consultation period. The second Town Hall was attended by approximately 800 industry and Government stakeholders across the 11 critical infrastructure sectors.
- **Out-of-session consultation**, including meetings with a number of stakeholders and email communication.
  - Stakeholders were encouraged to contact the Department out-of-session. The Department availed itself to stakeholders to discuss their concerns, working to ensure stakeholders’ understanding of the rules and the rules’ proportionality.
  - Out-of-session engagement also assisted in the iterative development of rules between workshops, through addressing concerns raised by individual stakeholders and proposing a solution.
  - This engagement strengthened the relationship between the Department and industry, while providing insights on implementation costs, entities’ operating environments and the overall impacts of the proposed regulatory changes.

  Mandatory Public Consultation, following the Minister commencing a 45-day consultation period on 5 October 2022 (the mandatory period is 28 days). Consultation included two Town Hall Sessions held on 10 October and 12 October 2022, attended by approximately 550 industry and Government stakeholders (across both sessions). The sessions provided information on the proposed RMP Rules as well as the broader obligation and supporting guidance material. At the meetings, the CISC provided information on the formal consultation process and the proposed RMP Rules, RMP Guidance, AusCheck background check for critical infrastructure, Protected Information Guidance and RMP Annual Report Submission form. Over the course of the 45-day consultation period the CISC held **four Q&A sessions** to hear the specific issues that industry raised.

The consultation roadmap on the RMP rules, pictured in Figure 4 below, provides additional insights on the topics for discussion at each consultation phase.

Figure 4: Consultation roadmap for RMP rules consultation



Outcomes and themes from consultation on RMP rules

The Department commenced the consultation process with a broad understanding of the business priorities and operational function of the responsible entities and their critical infrastructure asset.

From here, the Department adopted an approach to the RMP rules which developed over the course of the industry consultation period. This approach was to be adaptive and responsive to industry as the subject matter experts in their field, as well as maintaining an awareness of the economic, security and environmental impacts affecting their businesses from the subject matter expertise and understanding of the Department. The Department has always remained strongly aligned to the key objective of uplifting security and resilience of these critical infrastructure assets, and reiterated the necessity for these reforms due to the evolving risk and threat environment that Australia continues to face.

The Department initially began the design process for the RMP rules via sector-specific sessions, producing a set of draft rules which could be discussed and altered through in-depth workshops and out-of-session engagement. Following detailed consultation with the electricity sector over a five-month period, and in conjunction with the concurrent consultation with the gas, water, data and

payment systems asset classes, the Department identified significant commonalities across sectors regarding standards and principles, timing, and business impact.

Building on this consultation, having identified clear commonalities across critical infrastructure sectors, and acknowledging the clear call from industry to the PJCIS, the Department developed a set of sector-agnostic rules to sit across all sectors. The sector-agnostic rules amalgamated the standards and principles derived through engagement on sector-specific RMP rule hazard vectors into a consolidated and considered principles-based approach.

The sector agnostic RMP rules established a baseline threshold that all of industry could meet, which would ensure an overall uplift in the security and resilience of critical infrastructure assets in Australia. The Department provided industry with options to ensure that the RMP rules would be fit for purpose and adaptive for all responsible entities. The Department explained that this process would be iterative, and wanted to ensure that entities currently falling below the baseline threshold could meet the required obligations without a prohibitive cost to their business.

During consultation around the sector agnostic RMP rules, industry appreciated the need for a common approach to risk management across critical infrastructure sectors. There was also a general appreciation for the increased flexibility and certainty provided by the sector-agnostic rules, in response to feedback received from industry. Industry confirmed that the rules were implementable, and provided for baseline standards and principles to support the security and resilience of Australia's critical infrastructure. Industry was appreciative of the Government's commitment to working collaboratively to provide guidance material.

Table 21 *Key themes from consultation*

Rule category	Identified themes		Impact on development of rules
Sector-agnostic RMP rules	Information Sessions	• Industry believes the RMP rules provide a baseline for sector resilience and security. • There is an appetite for guidance material to support sector-specific uplift in security and resilience.	In response to feedback received during the information sessions, the Department committed to: • The development of guidance materials that would highlight aspects of risk management that should be prioritised by responsible entities, and assist industry in interpreting and implementing the rules to achieve an uplift in security and resilience.

The themes outlined in Table 21 demonstrate a continued receptiveness from industry for the RMP rules, and a continued desire to work in partnership with the Department to support the security and resilience of Australia's critical infrastructure.

Consultation on costs

Throughout consultation, industry was invited to provide feedback which would assist the Department in understanding the potential costs associated with the proposed RMP framework. Industry was informed that their insights would be used to assess the impact of the proposed reforms during the rules' development, and support the drafting of this RIS and its cost benefit analysis.

In the third workshop (for the electricity, gas, and water sectors) and second information session (for all remaining sectors), attendees were invited to participate in cost impact data collection through the completion of a cost impact template. This template was designed to collect substantive costing data to supplement the anecdotal costing discussions which had occurred throughout the workshop series. Industry was asked to provide:

- Their demographic information;
- Effort and cost estimates split by one-off and ongoing costs, staff effort, capital and other operating costs, and an estimated range between expected costs and highest possible costs; and
- Any comments on key boundaries, assumptions and cost drivers attached to the costing estimates provided.

Each asset class was provided with a cost impact template for completion, with submissions open for a period of four weeks.

The absence of entities within the sector that meet the definition of a small business indicated that consultation with the Australian Small Business and Family Enterprise Ombudsman was not required to identify expected costs to small businesses in preparing this RIS.[58]

Mandatory consultation period

Under the SLACIP Act, the Minister is required to publish a notice on the Department's website which contains draft RMP rules and invites industry stakeholders to make submissions. These submissions offer a further opportunity for feedback, which must be provided to the Minister within 28 days (or on another date of the Minister's choosing, in excess of the 28-day minimum consultation period) of the notice's publication. The Minister is required to consider any submissions received within this timeframe.

The Minister announced a 45-day consultation period on the proposed RMP Rules from 5 October – 18 November 2022. Among other things, the consultation period has included two Town Halls and four question and answer sessions. The majority of questions received were clarifying questions on the application of the Rules and the RMP obligation more broadly.

Roadmap for RMP rules consultation

Section 6 and 7 below outlines further avenues for discussion with, and for the provision of feedback from, industry, which would occur as part of the implementation and evaluation process for the proposed RMP framework.

[58] Guidance Note: Small Business, Office of Best Practice Regulation, 2021

6. Best option from those considered

6. Best option from those considered

The preceding consultation outcomes and analysis has demonstrated that **option 2: Mandatory RMP framework** is the most suitable option from those considered.

Section 3 of this RIS identified the objectives of Government action, as they relate to the RMP obligations contained in the SLACIP Act. These objectives align with, and seek to address, the elements of the problem discussed in Section 1. Table 22 below demonstrates that implementing the RMP framework for critical infrastructure assets will support each of Government's objectives for intervention and to comprehensively address the problems identified and discussed throughout this RIS:

***Table 22** Chosen option's alignment with problem and objectives*

Problem area	Government's objective	Why option 2?
There are risks to critical infrastructure assets.	• **Lower the material risk** of hazards and impacts of those hazards, as they manifest for critical infrastructure assets. • Ensure that adoption of the RMP for critical infrastructure assets is **reasonable and proportionate** to the purpose of the program.	✓ The introduction of the mandatory RMP framework under option 2 will directly address existing risks, and corresponding Government objectives, through: • Enabling, across all critical infrastructure assets, an uplift in security and resilience. The framework will establish a common baseline for critical infrastructure assets' security and resilience. Risk management practices, including preparedness, prevention, and mitigation, will become business as usual for all owners and operators of critical infrastructure assets. • Ensuring responsible entities identify, assess, and mitigate all hazards presenting a material risk to their critical infrastructure assets, in turn lowering the material risk of hazards and their subsequent impacts. • The introduction of a risk management program framework which ensures risks are considered and, where appropriate, addressed. This will enable the adoption of an all-hazards approach to risk management for critical infrastructure assets, increasing the resilience of these assets. Addressing these risks will result in substantial avoided costs for industry and the Australian economy, through mitigating the realisation of disruptive incidents to critical infrastructure assets. The range of avoided costs to critical infrastructure assets is across critical infrastructure assets, and is summarised in Section 4.2.2 and detailed in appendices S – CC. Extensive consultation on option 2 has ensured the framework remains reasonable and proportional, both in terms of costs and practical compliance activities.

Problem area	Government's objective	Why option 2?	
Existing legislative arrangements are insufficient for the current threat environment.	• **Lower the material risk** of hazards and impacts of those hazards, as they manifest for critical infrastructure assets. • **Avoid regulatory duplication** and facilitate a **coordinated uplift** in responsible entities' compliance with relevant standards.	✓	Option 2 addresses the insufficiency of existing legislative arrangements, and corresponding Government objectives, in a number of ways: • The RMP framework will introduce nuanced regulation, which acknowledges that industry is best placed to identify and lower the material risk of hazards, as they present to the responsible entity. This will result in avoided costs for industry, as well as avoided costs for the Australian economy as a whole. The size of the avoided costs varies between critical infrastructure assets and is summarised in Section 4.2.2 and detailed in appendices S – CC; and • The Framework's 'on switch' mechanism means it will not be imposed on assets already subject to a comparable, adequate regulatory scheme. This will ensure industry's compliance obligations are not duplicated and any unnecessary regulatory burden is avoided.
The Government has limited visibility of current risk management practices, and limited ability to ensure risks are appropriately managed across sectors.	• Improve Government's **visibility** over the security and resilience of critical infrastructure assets. • Provide Government with a range of graduated powers to support an uplift in resilience and security across Australia's critical infrastructure assets.	✓	The introduction of mandatory reporting requirements under option 2, including an annual report detailing the effectiveness of/compliance with an entity's RMP, will improve Government's visibility over the security and resilience of critical infrastructure assets, by providing Government with a clear visibility of each responsible entities' approach to uplifting the security and resilience of their asset/s. The risk management program framework will ensure risk management considerations are appropriately prioritised by responsible entities. Government will also have a range of graduated powers to support an uplift in resilience and security across Australia's critical electricity assets.
A stronger partnership between Government and industry is needed to drive a wholesale uplift in security and resilience.	• Avoid regulatory duplication and facilitate a **coordinated uplift** in responsible entities' compliance with relevant standards.	✓	The consultation process, involving collaboration between Government and industry and consultation on the manner and form of option 2, has marked the continuation of a strengthened partnership between Government and industry, leveraging the pre-existing relationships with some sectors through the TISN, and the engagements which commenced on the reforms in August 2020. Further, option 2's accompanying guidance materials and continued use of communication tools (including the TISN) will allow Government to strengthen its partnership with industry, by gaining an understanding of each asset's operating environment and each responsible entity's risk management practices. Similarly, a stronger partnership will ensure industry's awareness and understanding of the need to uplift the security and resilience of critical infrastructure assets has been enhanced.

The summary contained in Table 22 above indicates that option 2 is the best option. This is primarily because the introduction of a risk management program framework is the only option capable of addressing each problem area identified in this RIS, as described in Table 23 below. It achieves the objectives of Government intervention and stands to deliver substantial benefits to industry and the Australian economy as a whole. Conversely, Table 23 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 23** Option 1 and 3 lack of alignment with problem areas and Government objectives*

Problem area	Government's objective	Why not option 1 or 3?
There are risks to critical infrastructure assets.	• **Lower the material risk** of hazards and impacts of those hazards, as they manifest for critical infrastructure assets. • Ensure that adoption of the RMP for critical infrastructure assets is **reasonable and proportional** to the purpose of the program.	✖ **Option 1:** If the status quo is maintained, none of the identified existing risks or corresponding Government objectives can be met. This means: • There will be no common baseline for critical infrastructure assets' security and resilience, and a business-as-usual approach to risk management practices will not be achieved. • Responsible entities will not be compelled to identify and mitigate the material risk of hazards, or their subsequent impacts. • Organisations, and the economy as a whole, may incur substantial costs should disruptions affecting the operation of critical infrastructure assets occur. The severity and frequency of future disruptions and the associated whole-of-economy costs incurred varies between critical infrastructure assets. The potential costs of each incident are summarised in Section 4.2.1 and detailed in appendices S – CC.
		✖ **Option 3:** Under a voluntary arrangement, identified risks and associated Government objectives can only be addressed to the extent that responsible entities choose to participate in the framework. As a result: • There will be an inconsistent baseline for critical infrastructure assets' security and resilience, and a business-as-usual approach to risk management practices is unlikely to be achieved on a sector-wide basis. • Only some responsible entities will identify and mitigate the material risk of hazards and their subsequent impacts. • Organisations, and the economy as a whole, may incur substantial costs should disruptions affecting the operation of critical infrastructure assets occur. The severity and frequency of future disruptions and the associated whole-of-economy costs incurred varies between critical infrastructure assets. The potential costs of each incident are summarised in Section 4.2.3 and detailed in appendices S – CC.

Problem area	Government's objective	Why not option 1 or 3?	
Existing legislative arrangements are insufficient for the current threat environment.	• **Lower the material risk** of hazards and impacts of those hazards, as they manifest for critical infrastructure assets. • **Avoid regulatory duplication** and facilitate a **coordinated uplift** in responsible entities' compliance with relevant standards.	✖	**Option 1:** Status quo legislative arrangements do not provide nuanced regulations, which support entities in identifying and lowering the material risk of hazards. There would be no material uplift in risk management practices, or the security and resilience of critical infrastructure assets. Without concerted efforts to lower the material risk of 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. The costs will depend on an incident's frequency, severity and critical infrastructure assets affected. The potential costs of each incident are summarised in Section 4.2.1 and detailed in appendices S – CC.
		✖	**Option 3:** A voluntary framework means the material risk of hazards will only be lowered to the extent that organisations choose to participate in the framework. This will lead to an inconsistent uplift in responsible entities' compliance with relevant standards. Given the interconnected nature of critical infrastructure assets improvements to the security and resilience of such assets will be limited, where the framework is not implemented on a sector-wide, mandatory basis. Without concerted efforts to lower the material risk of 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. The costs will depend on an incident's frequency, severity and critical infrastructure assets affected. The potential costs of each incident are summarised in Section 4.2.3 and detailed in appendices S – CC.
The Government has limited visibility of current risk management practices and limited ability to ensure risks are appropriately managed across sectors.	• Improve Government's **visibility** over the security and resilience of critical infrastructure assets. • Provide Government with a range of graduated powers to support an uplift in resilience and security across Australia's critical infrastructure assets.	✖	**Option 1:** If the status quo is maintained, there will be no improvement to Government's visibility over the security and resilience of critical infrastructure assets, nor greater power for Government to act.
		✖	**Option 3:** If the framework is implemented on a voluntary basis, improvement to Government's visibility and graduated powers to support an uplift in resilience and security across critical infrastructure assets will be limited, as compliance with reporting requirements will not occur on a whole-of-sector basis.

Problem area	Government's objective	Why not option 1 or 3?	
A stronger partnership between Government and industry is needed to drive a wholesale uplift in security and resilience.	• Avoid regulatory duplication and facilitate a **coordinated uplift** in responsible entities' compliance with relevant standards.	✖	**Option 1:** Under the status quo, no additional mechanisms or discussion avenues will be created to strengthen the partnership between industry and Government. While the TISN will still be available for critical infrastructure entities, this substantially limits option 1's ability to facilitate a wholesale uplift in the security and resilience of critical infrastructure assets. Without concerted efforts to lower the material risk of 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. The costs will depend on an incident's frequency, severity and critical infrastructure assets affected. The potential costs of each incident are summarised in Section 4.2.1 and detailed in appendices S – CC.
		✖	**Option 3:** Under option 3, a stronger relationship may form between some industry stakeholders and Government. However, this will not be achieved on a sector-wide basis. While accompanying guidance material would be made available to critical infrastructure entities, regardless of their compliance with the voluntary framework, and continued use of TISN may facilitate communication, Government's understanding of each asset's operating environment and risk management practices will be limited. There would be inconsistent awareness and understanding among industry of the need to uplift the security and resilience of critical infrastructure assets. Given the interconnected nature of critical infrastructure assets, an inconsistent uplift in security and resilience across such assets may result in significant cost. Without concerted efforts to lower the material risk of 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. The costs will depend on an incident's frequency, severity and critical infrastructure assets affected. The potential costs of each incident are summarised in Section 4.2.1 and detailed in appendices S – CC.

As demonstrated in Table 22 and Table 23 above, options 1 and 3 are not capable of solving the policy problem, nor the Government objectives for intervention outlined by this RIS. Without implementing the RMP framework, as proposed by option 2, 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.

Although it offers the best option from those considered, option 2 is not without risks. Effective implementation of the RMP framework is essential for ensuring option 2's benefits are realised in their entirety. The risks associated with option 2, as well as a proposed implementation, monitoring and evaluation plan are discussed in Section 7 below.

7. Implementation and evaluation

7. Implementation and evaluation

This section outlines the Department's proposed implementation and evaluation plan, including an outline of key implementation tasks, and the challenges or risks associated with implementing the proposed RMP framework.

7.1. Implementation overview

Government's objectives for implementation are to introduce the RMP framework, in a manner which ensures affected industry stakeholders:

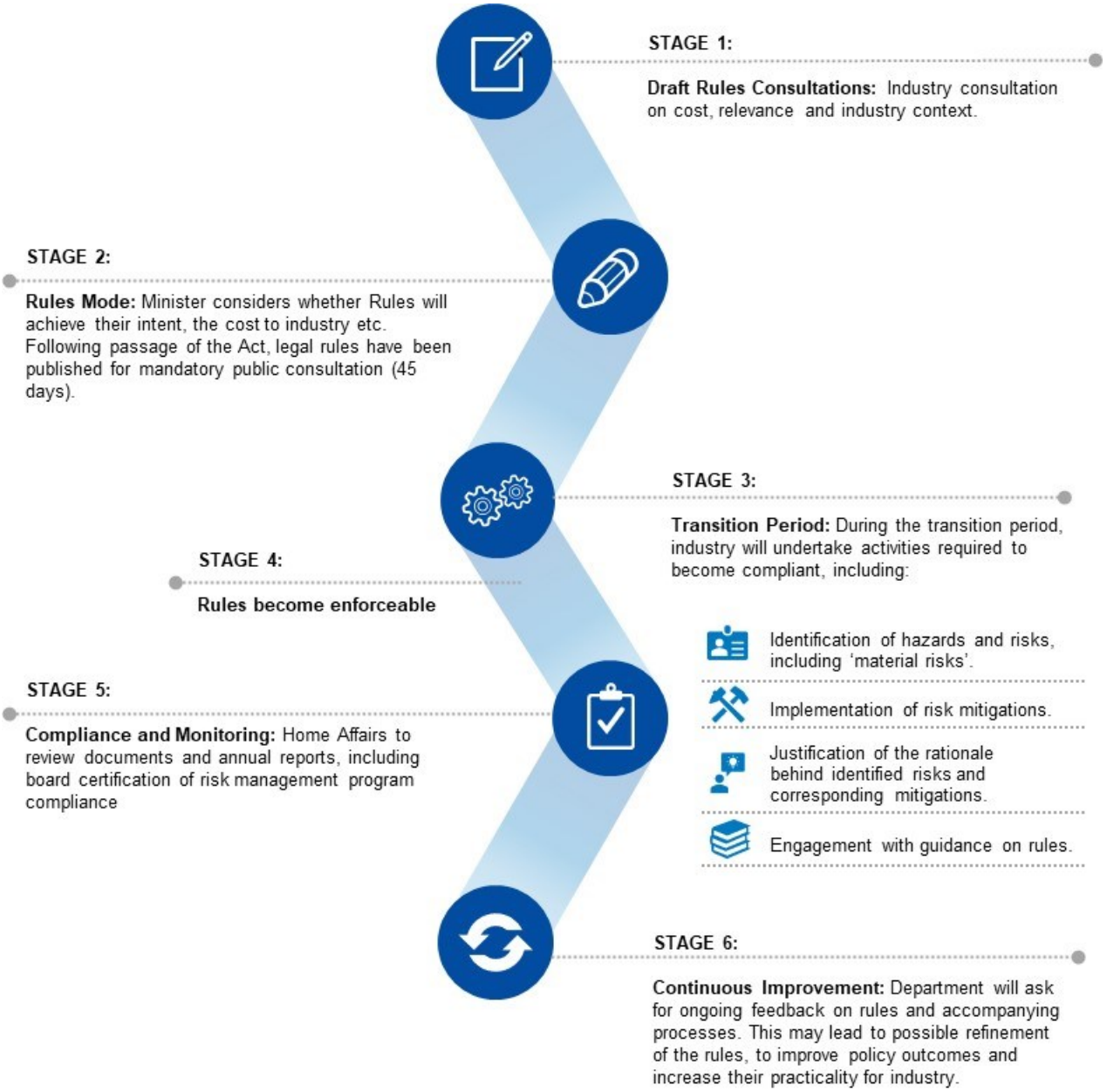
- Understand and comply with their obligations under the RMP;
- Engage with Government to identify, understand and mitigate risks which exist in the sector, and collaborate to drive the implementation of effective baseline security standards; and
- Receive appropriate and consistent direction, assistance, and guidance from Government, to allow for compliance with RMP obligations and support an uplift in security posture across the sector.

The Implementation Plan discussed below seeks to ensure these objectives are achieved.

7.1.1. Implementation plan

As outlined in Figure 5 below, the effective implementation of the RMP framework would be achieved through a six-stage implementation process. This includes the completion of the mandatory regulatory process, including public consultation on finalised, legal RMP rules, and a defined transition period.

***Figure 5**: Overview of Implementation Process*



Effective implementation would require the completion of several key activities across each of the six stages indicated in Figure 5 above. An overview of these activities is included in Table 24 below.

***Table 24** Key implementation activities*

Stage	Activity
Stage 1	Complete consultation with industry, including consultation on costing methodology, inputs, and outputs.
Stage 2	PJCIS review into SLACI Bill, PJCIS publication of outcomes and recommendations, and the Department's preparation of a Government response and proposed Government amendments. PJCIS review of the SLACIP Bill, PJCIS publication of outcomes and recommendations, and the Department's preparation of a Government response and proposed Government amendments.
	Passage of the SLACIP Act.
	Publication of legal, draft RMP rules for a minimum 28-day public consultation period. The mandatory consultation period has been undertaken over a 45-day.
	Preparation and publication of guidance material for industry on compliance with risk management plan obligations, which may include: • Case studies; • Frequently asked questions; • Threat information and risk advice through the enhanced TISN; • Insights into best practice and Government's expectations.
Stage 3	Rules made – Minister may 'switch on' RMP obligations for critical infrastructure assets, supported by finalised RMP rules.
	Commencement of transition period where industry begins to undertake activities to become compliant with RMP obligations, including by beginning to develop a RMP in line with Part 2A of the SLACIP Act.
	Preparation for enforcement of RMP obligations.
Stage 4	Enforcement of RMP obligations commences.
Stage 5	Post-implementation review of effectiveness and practicality of RMP obligations and rules for critical infrastructure assets, expected in 2026.
Stage 6	Implementation of formal and informal regular feedback mechanisms, with possible updates to guidance material and / or RMP rules in response.

7.1.2. Establishing regulatory functions

The Department's regulatory powers with respect to the SOCI Act arise from provisions in the *Regulatory Powers (Standard Provisions) Act 2014*. To implement the proposed RMP framework, the Department would discharge the relevant regulatory function (for all asset classes except critical payment systems). The 2021-22 Federal Budget announced that Government will commit $42.4 million over two years to improve security arrangements for critical infrastructure assets, in accordance with the SLACIP Act. This announcement meant additional funding would be available for the implementation of the RMP framework.

The Department will continue to engage and coordinate with existing regulators in the sector. For example, throughout the consultation and drafting of RMP rules, the Department has worked with the Reserve Bank of Australia to identify gaps in existing legislation, and ensure that the RMP rules are fit-for-purpose for the payment systems sector. Through this process it was determined that the Reserve Bank of Australia would be best placed to operate as the regulator, for the purposes of ensuring compliance with the SLACIP Act's RMP obligations across this asset class. All other relevant critical infrastructure assets will be regulated by the Department.

The Department would also work with Commonwealth agencies where the RMP framework will have a direct impact on those entities.

The Department will report on the implementation of the RMP obligations in its annual report to Parliament, in accordance with section 60 of the Act.

7.1.3. Compliance approach

The Department will support responsible entities in driving an uplift in asset security and resilience, through regulation and compliance. In doing so, it will work closely with the ACSC, responsible entities and industry regulators, to minimise regulatory duplication and cost to industry.

A strong and effective government-industry partnership is central to achieving the Australian Government's vision for critical infrastructure security and resilience. This partnership is supported by the Critical Infrastructure Resilience Strategy (CIRS) and the TISN – both non-regulatory measures. The Strategy is focussed on the continued operation of critical infrastructure in the face of all hazards. More resilient critical infrastructure will also help to support the continued provision of essential services (provided by critical infrastructure) to businesses, governments, and the community, as well as to other critical infrastructure sectors. The Government is currently in the process of updating the Strategy.

Government is currently updating the TISN, through expanding its sector groups and creating an online platform for engagement, which will support Federal, state and territory agencies and industry groups to work with critical infrastructure entities of all levels of maturity to deliver the Strategy's vision.

Draft regulatory principles

Regulatory functions and activities undertaken by the Department and its representatives may be guided by the following draft 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 adjust to respond to the nature and seriousness of non-compliance, and the potential risk to the security of Australian critical infrastructure.
- **Commitment to an industry and Government partnership.** The Department will work closely with industry and other government bodies, including TISN, National Emergency Management Agency, industry regulators and law enforcement agencies, to share threat information about security risk to Australia's critical infrastructure, and work collaboratively to monitor and ensure compliance functions.
- **Commitment to transparency and reporting on compliance action.** The SOCI Act requires the Minister for Home Affairs 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.

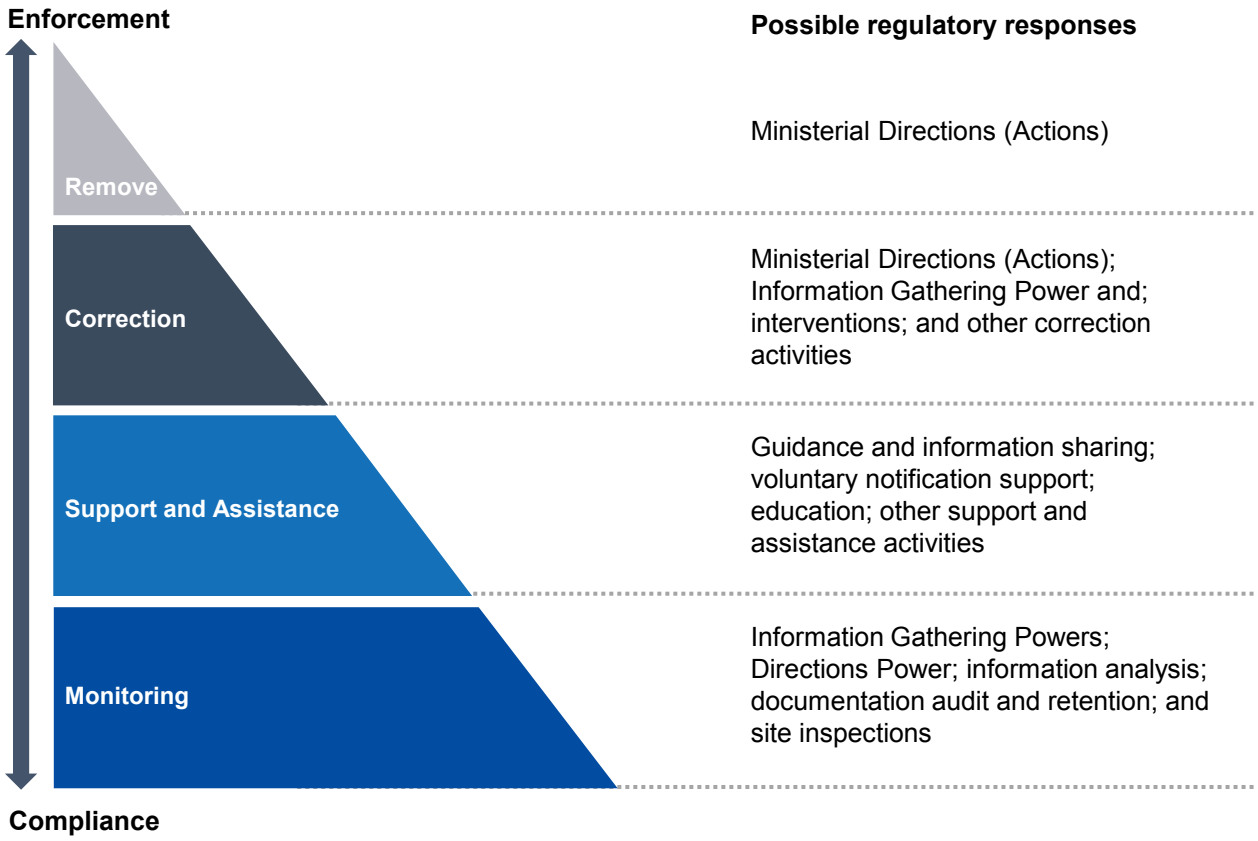
Possible regulatory responses

If responsible entities were to fail to comply with their obligations under the RMP, following the finalisation and 'switching on' of RMP obligations and the end of the transition period, such organisations may be subject to a regulatory response. The Department would work to educate and guide entities towards best practice security management, wherever possible, to encourage voluntary compliance. This would include educating responsible entities to ensure they understand their administrative and legislative obligations, as well as maintaining strong links with entities to promote ongoing best practice behaviours.

Figure 6 below outlines the Department's proposed approach to imposing regulatory responses, in the event of non-compliance with RMP obligations. The Department would use a tiered approach

to form its regulatory posture. Under this approach, regulatory actions and activities would be undertaken based on a scale ranging from support to penalties, proportionate to the nature and level of risk identified.

***Figure 6**: Compliance Strategy*



The Department would take a graduated approach to employing its enforcement powers, which may involve:

- Overseeing compliance with legislative obligations;
- Issuing reasonable requests for access to information, as well as inspection and audit powers;
- Issuing security notices which responsible entities must account for in their reporting;
- Issuing penalties for non-compliance; and
- Intervening and, where necessary, issuing directions where there are significant national security concerns which cannot be addressed through other means.

The Department would ensure that a penalty or intervention would only be imposed as a last resort, and in a manner proportionate to the risk presented by non-compliance.

Assessments of non-compliance

Assessments of non-compliance will be based on evidence, with an overall goal of consistency and fairness. When assessing non-compliance and determining an appropriate response, the Department will consider the following three factors:

1. **Risk** - What is the impact of non-compliance on Australia's national security? What is the nature of the risk? What solutions are available and how effective are they?
2. **Proportionality** - How serious is the risk? Are there any aggravating circumstances?

3. **Entity's Engagement** - What is the entity's attitude towards compliance? How cooperative is the entity, based on engagement with the Department and their compliance history?

7.2. Challenges and risks to implementation

There are several challenges and risks which could impede the Department's successful implementation of the RMP framework for critical infrastructure assets. These challenges and risks are identified in Table 25 below, and rated in terms of their likelihood and consequence, in accordance with Table 26.

***Table 25** Likelihood and consequence ratings*

Likelihood		Consequence	
Low	The identified risk or challenge would be 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 RMP framework.
Medium	It is reasonably possible that the identified risk or challenge would eventuate.	**Moderate**	If the identified risk or challenge does eventuate, it would have a substantial effect on the Department's ability to implement the RMP framework.
High	It is likely that the identified risk or challenge would evaluate.	**Severe**	If the identified risk or challenge does eventuate, it would have a significant effect on the Department's ability to implement the RMP framework.

***Table 26** Challenges and risks to implementation*

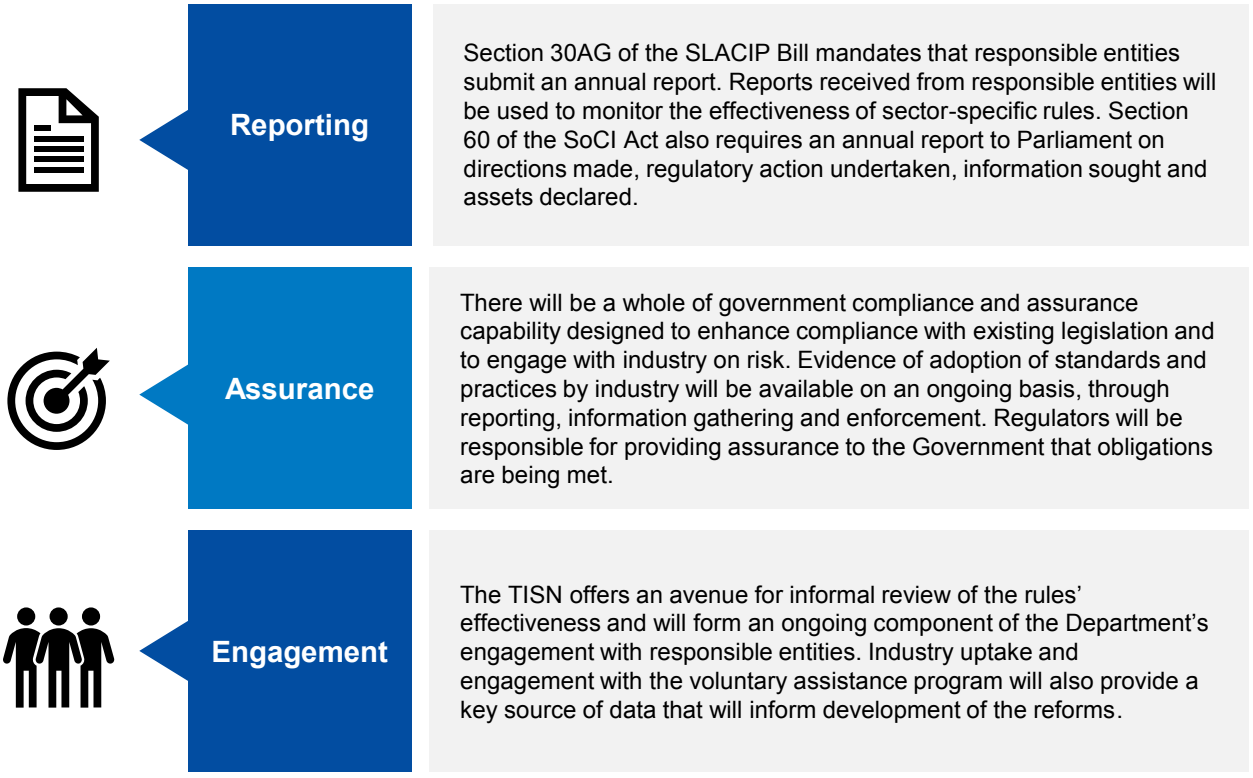
Challenge or risk	Likelihood	Consequence	Management
Lack of industry awareness of rules: Some industry stakeholders may be unaware of the RMP rules' implementation, or the extent of their obligations under the rules.	**Low**	**Severe**	The Department has led consultation with owners and operators of critical infrastructure assets, as part of the consultation process and to provide context on the impetus behind the proposed reforms. This consultation included town hall forums, a series of workshops, bilateral meetings, and open feedback forums. The Department also engaged with relevant peak bodies to notify their membership bases of the reforms. Consequently, it appears unlikely that any affected organisations would be unaware of the upcoming introduction of RMP rules. The 45-day consultation period provided a further opportunity to build industry's awareness of, and receive feedback on, the rules.
Lack of industry understanding as to Obligations: During consultation, some industry stakeholders indicated they lacked understanding of the rules' meaning and the extent of their obligations under the RMP.	**Medium**	**Moderate**	Consultation with industry aimed to provide clarity on the rules and activities required of stakeholders to comply with the RMP framework. Industry has had ongoing opportunities to provide additional feedback and ask questions. Further, following the finalisation of the rules, in the event of the rules' implementation industry would: • Be able to phone or email the Department on an as-needed basis; • Have access to guidance material published by the Department, to support industry in understanding their obligations under the

Challenge or risk	Likelihood	Consequence	Management
			RMP; and • Participate in a transitional period where industry would be encouraged to work towards meeting their RMP obligations without fear of consequences for non-compliance (a grace period).
Limited uptake: Where industry is unable to recognise the net-benefit associated with RMP rules (as it manifests as a whole-of-economy benefit, rather than a return on individual organisations' investments), industry uptake and cooperation may be affected.	**Low**	**Severe**	Consultation for RMP rules was a key initiative implemented to combat the potential for limited industry uptake and high implementation and compliance costs for industry. The Department has engaged widely to ensure industry support for the proposed regulatory changes to guide responsible entities towards meeting their new obligations. The inclusion of a 'grace period' in the Department's implementation plan would also support industry cooperation, sustained through ongoing, heightened engagement between Government and industry.
Government capability: The Department requires sufficient funding and staffing resources in order to efficiently implement the RMP rules and operate effectively as the regulator. Insufficient funding or understaffing could impact on the effectiveness of the proposed reforms.	**Medium**	**Severe**	The Department would undertake a significant recruitment campaign, followed by comprehensive training, 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. The staffing and funding requirements needed to effectively implement RMP obligations and subsequent rules would be provided to Government for consideration as soon as possible.
Implementation costs: There is a risk that the expected costs of implementation are either over or underestimated by industry and within this RIS.	**Medium**	**Moderate**	Requesting that industry include a compliance cost range when providing costing data (capturing both the expected cost and highest possible cost), has mitigated the risk that costs to industry could be higher than anticipated.

7.3. Monitoring and evaluation plan

The effectiveness of the RMP obligations would be assessed on an ongoing basis, including through the annual reports provided by responsible entities, Senate Estimate processes, and *ad-hoc* feedback from industry and Government stakeholders. Mechanisms for review of the RMP framework are outlined in Figure 7 below.

Figure 7: *Monitoring and review mechanisms*



7.3.1. Indicators of success

If the proposed RMP obligations were successful, Government, industry and the Australian public would have greater confidence in the resilience of our critical infrastructure providers, achieved through a measurable uplift in all-hazards risk management. Industry will strengthen their relationship with Government through heightened and more frequent bilateral engagement, an educative (rather than punitive) approach to compliance, and improved visibility for both industry stakeholders and Government. This will ensure all-hazard risks are identified, assessed, and mitigated, to support the sector's capacity to respond to a significant critical infrastructure disruption. These factors would be considered as part of the RMP's post-implementation review in 2026.

These indications of success align with Government's objectives for intervention, as set out in Table 27 below.

***Table 27** Alignment between Government objectives and outcomes*

Government's objective	Outcomes from RMP obligations
Lower the material risk of hazards and impacts of those hazards, as they manifest for critical infrastructure assets.	RMP obligations will lower the material risk of hazards and their impacts by inciting a sector-wide uplift in all hazards risk management.
Ensure that adoption of the RMP for critical infrastructure assets is **reasonable and proportional** to the purpose of the program.	Frequent bilateral engagement between industry and Government will ensure the reasonability and proportionality of the RMP. Further, Government's educative approach to compliance means regulatory responses to issues of non-compliance will be both reasonable and proportional.
Avoid regulatory duplication and facilitate a **coordinated uplift** in responsible entities' compliance with relevant standards.	The risk of regulatory duplication has been mitigated through the consultation process, encouraging industry to share existing applicable standards which may overlap with the proposed RMP obligations. The sector-wide application of the rules will facilitate a coordinated uplift across all critical infrastructure assets.
Improve Government's **visibility** over the security and resilience of critical infrastructure assets.	The practical requirements contained in RMP obligations (for example, annual reporting) will improve Government visibility. Further, visibility for both Government and industry will be supported through heightened and more frequent bilateral engagement.

Appendices

Appendix A: List of References

— (2015). Critical Infrastructure Resilience Strategy: Plan. https://cicentre.gov.au/document/P50S021.

— (2020). Widespread and Long Duration Outages - Values of Customer Reliability Consultation Paper. March.

— (2021). Draft Critical Infrastructure Asset Definition Rules. Home Affairs. https://www.homeaffairs.gov.au/reports-and-pubs/files/critical-infrastructure-asset-definition-rules-paper.pdf

— (2021). Safeguarding Critical Infrastructure. https://cisc.gov.au/infrastructure.

— (n.d). Trusted Information Sharing Network. https://cicentre.gov.au/tisn.

—. (2017). Australian Cyber Security Centre Threat Report. https://www.cyber.gov.au/sites/default/files/2019-03/ACSC_Threat_Report_2017.pdf.

—. (2020). Security Coordination - Critical Infrastructure Resilience. 23 April. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/critical-infrastructure-resilience.

—. (2020). Security Legislation Amendment (Critical Infrastructure) Bill 2020: Explanatory Document. Critical Infrastructure Centre. https://www.homeaffairs.gov.au/reports-and-pubs/files/exposure-draft-bill/exposure-draft-security-legislation-amendment-critical-infrastructure-bill-2020-explanatory-document.pdf.

—. (2021). Federal Budget 2021-22, Budget Paper No. 2, Part 2: Payment Measures. https://budget.gov.au/2021-22/content/bp2/download/bp2_03_payment.pdf.

—. (2021). Protecting Critical Infrastructure and Systems of National Significance: Governance Rules - Risk Management Program.

—. (2021). Major banks' online services, airline systems go down. *Itnews.* https://www.itnews.com.au/news/major-banks-online-services-eftpos-airline-systems-go-down-566080

—. (n.d). About Financial Market Infrastructure. https://www.rba.gov.au/payments-and-infrastructure/financial-market-infrastructure/about.html

—. (2015). Critical Infrastructure Resilience Strategy: Plan. https://cicentre.gov.au/document/P50S021.

—. (2018). AEMO Request for Protected Event Declaration: Potential Loss of Multiple Generators in South Australia. November.

—. (2019). Cyber security continues to be a key focus for the energy industry. *AEMO*. https://aemo.com.au/newsroom/media-release/cyber-security-key-focus-for-the-energy-industry, 1 August.

—. (2020). Ransomware in Australia. *Australian Signals Directorate*. https://www.cyber.gov.au/sites/default/files/2020-10/Ransomware%20in%20Australia%20%28October%202020%29.pdf.

—. (2020). Security Coordination - Critical Infrastructure Resilience. 23 April. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/critical-infrastructure-resilience.

—. (2021). Australia Energy Sector Cyber Security Framework Education Workshop. Australian Energy Market Operator. 30 June. Accessed August 3, 2021. https://aemo.com.au/-/media/files/initiatives/cyber-security/2021/the-2020-21-aescsf-education-workshop-pack.pdf?la=en.

—. (2021). Protecting Critical Infrastructure and Systems of National Significance - Co-design of Governance Rules: Critical Infrastructure Risk Management Program, Summary of Consultation. https://www.homeaffairs.gov.au/reports-and-pubs/files/co-design-governance-rules-risk-management-summary.pdf.

—. (2021). Safeguarding Critical Infrastructure. https://cicentre.gov.au/infrastructure.

—. (n.d). Trusted Information Sharing Network. https://cicentre.gov.au/tisn.

ABC. (2021). Colonial Pipeline says operations back to normal as US blames Darkside for ransomware attack. *ABC*. https://www.abc.net.au/news/2021-05-16/colonial-pipeline-normal-operations-ransomeware-attack/100142608

ABC. (2021) Hackers demand $92m in bitcoin for data stolen during attack on US IT company Kaseya. *ABC.* https://www.abc.net.au/news/2021-07-06/hackers-demand-92m-after-gargantuan-ransomware-attack/100269678

Abelson, P. (2007). Establishing a Monetary Value for Lives Saved: Issues and Controversies, Working Papers in Cost benefit Analysis WP 2008-2. Department of Finance and Deregulation. https://www.pmc.gov.au/sites/default/files/publications/Working_paper_2_Peter_Abelso n.pdf

Abrams, L. (2021). Trucking giant Forward Air reports ransomware data breach. *Bleeping Computer.* https://www.bleepingcomputer.com/news/security/trucking-giant-forward-air-reports-ransomware-data-breach/ 21 December.

AEMC. (2019). "Definition of Unserved Energy, Final Report. August.

AEMC. (n.d). Electricity Market. AEMC. https://www.aemc.gov.au/energy-system/electricity/electricity-market.

Aid & International Development Forum. (2017). 5 Reasons Why Everyone Needs Clean Drinking Water. http://www.aidforum.org/topics/health-and-wash/5-reasons-why-everyone-needs-clean-drinking-water/ 14 December

Alinta Energy. (2020). Response to Exposure Draft - Security Legislation Amendment (Critical Infrastructure) Bill 2020. 27 November.

Anderson, Rob. (2020). "Brad Flanagan, Essential Energy's Head of Cybersecurity, on securing OT environments and the AESCSF." PSC Consulting, Brad Flanagan, Essential Energy's Head of Cybersecurity, on securing OT environments and the AESCSF - PSC Consulting 16 December.

AP News. (2020). German hospital hacked, patient taken to another city dies. *AP News.* 18 September. https://apnews.com/article/technology-hacking-europe-cf8f8eee1adcec69bcc864f2c4308c94.

Arcadia. (2017). Causes and Effects of Water Scarcity and Droughts. https://blog.arcadia.com/causes-and-effects-of-water-scarcity/ 14 December.

Ascierto, R. (2021). Data Center Insecurity. *Data Center Dynamics*. https://www.datacenterdynamics.com/en/opinions/data-center-insecurity/, 13 April.

Atlantic Council. (2018). Managing risk in the energy sector's cyber supply chain. *World Economic Forum.* https://www.weforum.org/agenda/2018/06/managing-risk-in-the-energy-sector-s-cyber-supply-chain/, 16 June.

Atlassian. (2020). November 27. Atlassian's Submission in relation to the Security Legislation Amendment (Critical Infrastructure) Bill 2020. Atlassian. https://www.homeaffairs.gov.au/reports-and-pubs/files/critical-infrastructure-consultation-submissions/EDS035-CISoNS-Atlassian.PDF.

AuDA. (2021). AuDA's Terms of Endorsement. https://www.auda.org.au/about-auda/governance/terms-endorsement.

Ausgrid. (2020). Response to Exposure Draft - Security Legislation Amendment (Critical Infrastructure) Bill 2020. 27 November.

Australian Border Force. (2021). Maritime Border Command. https://www.abf.gov.au/about-us/what-we-do/border-protection/maritime.

Australian Energy Market Operator. (2018). AEMO Report: Cyber security preparedness in the NEM and WEM. *AEMO*. https://aemo.com.au/en/newsroom/media-release/cybersecurity-in-the-nem-and-wem.

Australian Energy Market Operator. (2018) AEMO Request for Protected Event Declaration: Potential Loss of Multiple Generators in South Australia.

Australian Energy Market Operator. (2019) Cyber security continues to be a key focus for the energy industry. *AEMO*. https://aemo.com.au/newsroom/media-release/cyber-security-key-focus-for-the-energy-industry.

Australian Energy Market Operator. (2021). Australia Energy Sector Cyber Security Framework Education Workshop. Australian Energy Market Operator: https://aemo.com.au/-/media/files/initiatives/cyber-security/2021/the-2020-21-aescsf-education-workshop-pack.pdf?la=en

Australian Energy Market Operator. (2018). AEMO Report: Cyber security preparedness in the NEM and WEM. AEMO. https://aemo.com.au/en/newsroom/media-release/cybersecurity-in-the-nem-and-wem, 20 December.

Australian Energy Regulator. (2020) Widespread and Long Duration Outages - Values of Customer Reliability Consultation Paper.

Australian Energy Regulator. (2018). Investigation Report into South Australia's 2016 State-wide Blackout. Australian Energy Regulator. https://www.aer.gov.au/wholesale-markets/compliance-reporting/investigation-report-into-south-australias-2016-state-wide-blackout.

Australian Financial Review. (2021). Frontier Software payroll company Hacked. *Australian Financial Review* https://www.afr.com/work-and-careers/workplace/pay-in-crisis-as-major-payroll-company-hacked-20211117-p599mr.

Australian Government. (2021). Federal Budget 2021-22, Budget Paper No. 2, Part 2: Payment Measures. https://budget.gov.au/2021-22/content/bp2/download/bp2_03_payment.pdf.

Australian Government Department of Infrastructure, Transport, Regional Development and Communications. 2021. Terms of Endorsement for AuDA. November. https://assets.auda.org.au/a/2021-11/Terms%20of%20Endorsement%20for%20auDA%20%282021%29.pdf?VersionId=xq7v3.5kGRr.UnneJtHDhGUVaWJKc231.

Australian Government Productivity Commission. (2021). Vulnerable Supply Chains. Productivity Commission Interim Report. March. https://www.pc.gov.au/inquiries/current/supply-chains/interim/supply-chains-interim.pdf.

Australian Security Intelligence Organisation. (2019). ASIO Annual Report. https://www.asio.gov.au/sites/default/files/ASIO%20Annual%20Report%202019-20.pdf.

Australian Security Intelligence Organisation. (2021). ASIO Annual Report. https://www.asio.gov.au/sites/default/files/Annual%20Report%202020-21%20WEB.pdf.

Australian Signals Directorate. (2017). Australian Cyber Security Centre Threat Report. Retrieved from https://www.cyber.gov.au/sites/default/files/2019-03/ACSC_Threat_Report_2017.pdf.

Australian Signals Directorate. (2020). Ransomware in Australia. Canberra: Australian Signals Directorate. https://www.cyber.gov.au/sites/default/files/2020-10/Ransomware%20in%20Australia%20%28October%202020%29.pdf.

Australian Signals Directorate. (2020). Australian Cyber Security Centre Annual Cyber Threat Report 2019-2021. https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf.

Australian Signals Directorate. (2021). ACSC Annual Cyber Threat Report – 1 July 2021 to 30 June 2021. https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21.

Barrera, A. Parraga. M. (2021). “Eye of fire” in Mexican waters snuffed out, says national oil company. *Reuters.* https://www.reuters.com/business/energy/fire-offshore-pemex-platform-gulf-mexico-under-control-2021-07-02/.

BBC News. (2017). NotPeyta cyber-attack cost TNT at least $300m. https://www.bbc.com/news/technology-41336086 21 December.

BBC News. (2010). Australia: Queensland floods spur more evacuations. https://www.bbc.com/news/world-asia-pacific-12097280

Bennetto, J. (1997). How the IRA plotted to switch off London. *The Independent*. 11 April.

Bloomberg. (2021). Hackers Breached Colonial Pipeline Using Compromised Password. Technology Cybersecurity. Colonial Pipeline Cyber Attack: Hackers Used Compromised Password – Bloomberg.

Bloomberg. (2021). U.K. Road-Fuel Panic Deepens in the Pain in Crisis-Prone Economy. *Bloomberg* https://www.google.com/search?q=U.K.+Road-Fuel+Panic+Deepens+the+Pain+in+Crisis-Prone+Economy+-+Bloomberg&oq=U.K.+Road-Fuel+Panic+Deepens+the+Pain+in+Crisis-Prone+Economy+-+Bloomberg&aqs=edge.69i57.458j0j4&sourceid=chrome&ie=UTF-8&safe=active&ssui=on.

Branigan, T. (2011). Tsunami, earthquake, nuclear crisis - now Japan faces power cuts. *The Guardian*. 14 March. https://www.theguardian.com/world/2011/mar/13/japan-tsunami-earthquake-power-cuts.

Brill, A. B. L. (2021). Does a Ransomware Attack Constitute a Data Breach? *Duff & Phelps*. https://www.kroll.com/en/insights/publications/cyber/ransomware-attack-constitute-data-breach.

BSA The Software Alliance. (2020). CRITICAL INFRASTRUCTURE BILL — BSA COMMENTS. https://www.homeaffairs.gov.au/reports-and-pubs/files/critical-infrastructure-consultation-submissions/EDS038-CISoNS-BSATheSoftwareAlliance.PDF.

Butts, T. (2021). Sinclair Still Dealing with Effects from Ransomware Attack. *TV Technology*. 4 November. https://www.tvtechnology.com/news/sinclair-still-dealing-with-effects-from-ransomware-attack

Callen, T. (2020). "Gross Domestic Product: An Economy's All." International Monetary Fund, https://www.imf.org/external/pubs/ft/fandd/basics/gdp.htm 21 December

Callinan, Rory. (2021). Queensland water supplier Sunwater targeted by hackers in months-long undetected cyber security breach. *ABC News*. https://www.abc.net.au/news/2021-11-11/qld-hackers-target-water-supplier-sunwater-cyber-security-attack/100610400 16 December.

Centers for Disease Control and Prevention. n.d. Malaria: The Disease. https://www.cdc.gov/malaria/about/faqs.html 16 December.

Chapman, A. (2019). Myer's EFTPOS machines crash across the country amid Boxing Day chaos. *7 News*. https://7news.com.au/lifestyle/shopping/myers-eftpos-machines-crash-across-the-country-amid-boxing-day-chaos-c-622096.

Chenneveau, D. (2020). A resilient return for Asia's manufacturing and supply chains? 1 June. https://www.mckinsey.com/business-functions/operations/our-insights/a-resilient-return-for-asias-manufacturing-and-supply-chains.

Cimpanu, C. (2020). Google says it mitigated a 2.54 Tbps DDoS attack in 2017, largest known to date. *ZDNet.* https://www.zdnet.com/article/google-says-it-mitigated-a-2-54-tbps-ddos-attack-in-2017-largest-known-to-date/.

Cockburn P. (2019). Journalists with leaked documents treated like they have 'stolen goods', ABC boss says. *ABC News*. 13 August. https://www.abc.net.au/news/2019-08-13/press-freedom-inquiry/11407624.

Colangelo, A. (2019). Gift cards declined on Boxing Day at Myer and Coles. *The Sydney Morning Herald.* https://www.smh.com.au/business/consumer-affairs/gift-cards-declined-on-boxing-day-at-myer-and-coles-20181226-p50obp.html.

Collier, R. (2017). NHS ransomware attack spreads worldwide. *CMAJ.* https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5461132/.

Corera, G. (2016). How France's TV5 was almost destroyed by 'Russian hackers'. *SBS News*. 10 October. https://www.bbc.com/news/technology-37590375.

Cotton, B. 2021. What does the fuel crisis mean for the UK economy?. *Business Leader.* https://www.businessleader.co.uk/what-does-the-fuel-crisis-mean-for-the-uk-economy/.

Council, Y. E. 2021. 10 Data Security Risks That Could Impact Your Company In 2020. *Forbes.* https://www.forbes.com/sites/theyec/2019/10/01/10-data-security-risks-that-could-impact-your-company-in-2020/?sh=31a7a1e0a0c0.

Critical Infrastructure Centre. (2015). Critical Infrastructure Resilience Strategy. *CISC.* https://www.cisc.gov.au/help-and-support-subsite/Files/critical_infrastructure_resilience_strategy_plan.pdf.

Critical Infrastructure Centre. (n.d.) Critical Infrastructure Centre Compliance Strategy. https://www.cisc.gov.au/help-and-support-subsite/Files/critical-infrastructure-centre-compliance-strategy.pdf 16 December.

CRO Forum. (2011). Power Blackout Risks – Risk Management Options, Emerging Risk Initiative – Position Paper. November. https://www.preventionweb.net/files/24128_powerblackoutrisks1.pdf.

Crozier, R. (2018). NAB outage caused by power cut to mainframe. *IT News.* Itnews.https://www.itnews.com.au/news/nab-outage-caused-by-power-cut-to-mainframe-491780.

Cyber and Infrastructure Security Centre. (2015). Critical Infrastructure Resilience Strategy: Plan. https://www.cisc.gov.au/help-and-support-subsite/Files/critical_infrastructure_resilience_strategy_plan.pdf.

Cyber and Infrastructure Security Centre. (2021). Safeguarding Critical Infrastructure. https://cicentre.gov.au/infrastructure.

Dawn-Hiscox, T. (2017). Houston data centers withstand Hurricane Harvey. *DCD.* https://www.datacenterdynamics.com/en/news/houston-data-centers-withstand-hurricane-harvey/

Deloitte. (2020). Understanding the sector impact of COVID-19 - Oil, Gas & Chemicals. *Deloitte*. 1 April.

Denniss, Paul Read and Richard. (2020). With costs approaching $100 billion, the fires are Australia's costliest natural disaster. *The Conversation*. 17 January. https://theconversation.com/with-costs-approaching-100-billion-the-fires-are-australias-costliest-natural-disaster-129433.

Department of Environment and Energy. (2019). Liquid Fuel Security Review Interim Report. https://www.energy.gov.au/sites/default/files/liquid-fuel-security-review-interim-report.pdf.

Department of Home Affairs. (2020). Security Coordination - Critical Infrastructure Resilience. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/critical-infrastructure-resilience.

Department of Home Affairs. (2020). Submission on Protection of Critical Infrastructure and Systems of National Significance. *New Payments Platform.* New Payments Platform submission on Protecting Critical Infrastructure and Systems of National Significance (homeaffairs.gov.au).

Department of Home Affairs. (2021). Protecting Critical Infrastructure and Systems of National Significance - Co-design of Governance Rules: Critical Infrastructure Risk Management Program, Summary of Consultation". https://www.homeaffairs.gov.au/reports-and-pubs/files/co-design-governance-rules-risk-management-summary.pdf.

Department of Home Affairs. (2021). Protecting Critical Infrastructure and Systems of National Significance: Governance Rules - Risk Management Program.

Department of Home Affairs. (2020). Regulation Impact Statement (RIS). https://obpr.pmc.gov.au/sites/default/files/posts/2020/12/ci_sons_regulation_impact_statement_-_final_second_pass.pdf 21 December.

Department of Home Affairs. (2020). Security Coordination - Critical Infrastructure Resilience. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/critical-infrastructure-resilience.

Department of Home Affairs. (2021). Protecting Critical Infrastructure and Systems of National Significance. Draft Critical Infrastructure Asset Definition Rules. https://www.homeaffairs.gov.au/reports-and-pubs/files/critical-infrastructure-asset-definition-rules-paper.pdf.

Department of Home Affairs. (2021). Protecting Critical Infrastructure and Systems of National Significance - Co-design of Governance Rules: Critical Infrastructure Risk Management Program, Summary of Consultation. https://www.homeaffairs.gov.au/reports-and-pubs/files/co-design-governance-rules-risk-management-summary.pdf.

Department of Prime Minister and Cabinet. (2020). Regulatory Burden Measure Framework. *Department of Prime Minister and Cabinet*. March. https://pmc.gov.au/sites/default/files/publications/regulatory-burden-measurement-framework-2.pdf.

Dignan, L. (2017). FedEx said TNT Peyta attack financial hit will be material, some systems won't come back. *ZDNet.* https://www.zdnet.com/article/fedex-said-tnt-petya-attack-financial-hit-will-be-material-some-systems-wont-come-back/ 21 December.

Din, A. (2021). "Forward Air Corporation Recently Disclosed Data Theft Following a Ransomware Attack." Heimdal Security, https://heimdalsecurity.com/blog/forward-air-corporation-recently-disclosed-data-theft-following-a-ransomware-attack/ 21 December.

Divjak, C. (1998). Sydney's water crisis – a systemic failure. *World Socialist Web Site.* https://www.wsws.org/en/articles/1998/09/syd-s11.html.

Ernst & Young. (2016). Managing Insider Threat. https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/assurance/assurance-pdfs/EY-managing-insider-threat.pdf.

Fachot, M. (2019). Cyber security – a priority for broadcasters and media companies. *E Tech.* 15 January.

Ferguson, J. (2021). Diesel crisis threatens to crash supply chain. *The Australian*. 2 December. https://www.theaustralian.com.au/nation/politics/diesel-crisis-threatens-to-crash-supply-chain/news-story/a11f93b9605cbe9d921f089242ab9619

Foley, N and M. (2020). Energy grid under threat as bushfires bear down on power lines. *The Sydney Morning Herald.* https://www.smh.com.au/business/the-economy/energy-grid-under-threat-as-bushfires-bear-down-on-power-lines-20200103-p53om1.html.

Fortress. (2020). “Healthcare Under Cyber-Attack: Prevention is the Best Medicine”. https://fortresssrm.com/healthcare-under-cyber-attack-prevention-is-the-best-medicine/.

Fruhlinger, J. (2021). DDoS explained: How distributed denial of service attacks are evolving. *CSO Australia*.

Galeon, D. (2016). DDoS Attack: What Friday’s Massive Internet Outage Was All About. *Futurism*. https://futurism.com/ddos-attack-what-fridays-massive-internet-outage-was-all-about.

Gambrell, J. (2021). Cyber-attack closes Iran’s petrol stations. *7 News*. https://7news.com.au/technology/security/cyber-attack-closes-irans-petrol-stations-c-4340647

Giles, Ma. (2019). Triton is the world's most murderous malware, and it's spreading. *MIT Technology Review*. https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/.

Google Cloud. (2021). Google Cloud Status Dashboard. https://status.cloud.google.com/incidents/8DhiwfKvD987f5tJrj1G.

Gordon, A. (2016). The Official (ISC)2 Guide to the CCSP CBK (2nd ed.) [E-book]. Sybex. Sybex: The Official (ISC)2 Guide to the CCSP CBK, 2nd Edition - Adam Gordon (wiley.com).

Government, Australian. (n.d.) Chapter 2: Natural Disaster Risk. Royal Commission into National Natural Disaster Arrangements. https://naturaldisaster.royalcommission.gov.au/publications/html-report/chapter-02.

Greenberg, A. (2019). Cyberspies Hijacked the Internet Domains of Entire Countries. *Wired.* https://www.wired.com/story/sea-turtle-dns-hijacking/.

Gupta, S., & Dias, A. (2021). The Google Cloud region in Melbourne is now open. *Google Cloud Blog.* https://cloud.google.com/blog/products/infrastructure/the-google-cloud-region-in-melbourne-is-now-open.

GXI Volume 4 Archives - Interconnections - The Equinix Blog. (2021). Equinix. https://blog.equinix.com/blog/tag/gxi-volume-4/.

Hope, Z. (2021). The peculiar reason hackers invaded one of Queensland’s biggest water companies. Brisbane Times, https://www.brisbanetimes.com.au/national/queensland/the-peculiar-reason-hackers-invaded-one-of-queensland-s-biggest-water-companies-20211111-p5987b.html.

Hurley, D. (2021). Panted Viruses Threat: ASIO fears sabotage. *Sunday Herald Sun*. 1 August.

Hurst, D. (2011). Three quarters of Queensland a disaster zone. *Brisbane Times.* January 11.

IBIS World. (2021). Fossil Fuel Electricity Generation in Australia. *IBIS World*. https://my.ibisworld.com/au/en/industry/d2611/about.

IBIS World. (2021). Electricity transmission in Australia. *IBIS World*. https://my.ibisworld.com/au/en/industry/d2620/about.

IBM. (2021). Cost of a Data Breach Report 2021. *IBM Security*. https://www.ibm.com/downloads/cas/OJDVQGRY.

Insurance Council of Australia. (2011). Flooding in the Brisbane River Catchment; ICA Hydrology Panel: Sydney, Australia, 20 February 2011.

Johnson, Dr S. (2017). You don't know the power of the Dark Side. 14 September. https://www.energynetworks.com.au/news/energy-insider/you-dont-know-the-power-of-the-dark-side/#_ftn1.

Jones, N. (2021). FULL LIST: All the roads closed in South East Queensland. *The Courier Mail*. https://www.couriermail.com.au/news/emergency-services/full-list-all-the-roads-closed-in-south-east-queensland/news-story/006ab66784619084a82ad4c1569907c9 21 December.

Jowitt, T. (2019). Human Error Blamed For Visa Data Breach Down Under. *Silicon UK.* https://www.silicon.co.uk/security/cyberwar/visa-data-breach-down-under-279407.

Katz, J. (2021). Survey shows many water utilities struggle with cybersecurity. GCN. https://gcn.com/cybersecurity/2021/06/survey-shows-many-water-utilities-struggle-with-cybersecurity/315479/.

Kilpatrick, J. (2021). COVID-19: Managing supply chain risk and disruption. *Deloitte.* https://www2.deloitte.com/global/en/pages/risk/cyber-strategic-risk/articles/covid-19-managing-supply-chain-risk-and-disruption.html.

Kohen, I. (2019). 10 Data Security Risks That Could Impact Your Company In 2020. *Forbes*. https://www.forbes.com/sites/theyec/2019/10/01/10-data-security-risks-that-could-impact-your-company-in-2020/?sh=67100144a0c0.

KPMG. (2020). The Pace of Change - IT / OT Convergence. *KPMG.* https://home.kpmg/content/dam/kpmg/be/pdf/2020/06/it-ot-cybersec-convergence.pdf.

Lannin, S. (2021). ACCC launches investigations into 'exorbitant' shipping and port charges. *ABC News*. https://www.abc.net.au/news/2021-09-14/prices-ports-transport-shopping-accc-covid-inflation/100458836 .

Lauder, S. Reardon, A. McCutcheon. J. (2020). ABC's south coast transmitter that melted during Black Summer bushfired back in action. *ABC News*. 30 October. https://www.abc.net.au/news/2020-10-30/abc-radio-transmitter-melted-in-nsw-bushfires-back-in-action/12830154

Lewis, L. (n.d.) Cholera, Dengue Fever, and Malaria: The Unquestionable Link to Water. *The Water Project.* https://thewaterproject.org/water-scarcity/cholera-dengue-fever-malaria-water.

Litton, E. Huckson, S, e al. (2020). Surge capacity of intensive care units in case of acute increase in demand caused by COVID-19 in Australia. *Med J Australia*. https://www.mja.com.au/journal/2021/215/11/increasing-icu-capacity-accommodate-higher-demand-during-covid-19-pandemic *212*, 463-467.

Lord, N. (2020). The cost of a malware infection? For Maersk, $300 million" *Digital Guardian*. https://digitalguardian.com/blog/cost-malware-infection-maersk-300-million.

Lyne, M. (2020). Building our nation's climate and disaster resilience: where to from here?. *Commonwealth Scientific and Industrial Research Organisation.* https://ecos.csiro.au/building-climate-and-disaster-resilience/.

Matthews, K.L. (2021). What to know about the main causes of inflation. *Business Insider Australia*, https://www.businessinsider.com.au/causes-of-inflation?r=US&IR=T 21 December

McDonald, T. (2019, 20 December). Australia fires: The huge economic cost of Australia's bushfires. *BBC News.* 20 December. https://www.bbc.com/news/business-50862349.

McDonald, T. (2020, 10 December). Cost of cyber-attack revealed as Barwon Health records surplus in challenging year'. *Geelong Advertiser.* https://www.geelongadvertiser.com.au/news/geelong/cost-of-cyber-attack-revealed-as-barwon-health-records-surplus-in-challenging-year/news-story/625fa8fc13778725cfc54e9acb79d8fe

McKinnell, J. (19 September). Shen Neng 1 reef spill leads to $39 million payout six years on. *The New Daily*. https://thenewdaily.com.au/news/national/2016/09/19/shen-neng-oil-spill-payout/

McLaughlin, K. (2020, 7 January). Australian babies are being born in smoke-filled hospitals as hundreds of bushfires burn across the country. *Insider*. https://www.insider.com/australian-bushfires-babies-delivered-in-smoky-hospitals-2020-1

Michaelson, R. (2021). Ever Given released from Suez Canal after compensation agreed. *The Guardian*. https://www.theguardian.com/world/2021/jul/07/ever-given-released-from-suez-canal-after-compensation-agreed 21 December

Moore, T. (2016, 7 May). Costs to remove toxic paint from Great Barrier Reef 'triples' to $141 million. *Brisbane Times*. https://www.brisbanetimes.com.au/national/queensland/costs-to-remove-toxic-paint-from-great-barrier-reef-triples-to-141-million-20160506-gooe84.html

Morrow, T. (2018). 12 Risks, Threats, & Vulnerabilities in Moving to the Cloud. *SEI Blog*. https://insights.sei.cmu.edu/blog/12-risks-threats-vulnerabilities-in-moving-to-the-cloud/

Moss, S. (2021, 25 August). Google Cloud hit by outage in new Melbourne, Australia, region. *Data Center Dynamics*. https://www.datacenterdynamics.com/en/news/google-cloud-hit-by-outage-in-new-melbourne-australia-region/

Motherwell, S. (2018). NAB outage: Bank promises to compensate customers for losses from nationwide disruption. *ABC News.*

Murphy, K. (2017, 10 February). Electricity market operator denies being 'asleep at the wheel' during blackout. *The Guardian*. https://www.theguardian.com/australia-news/2017/feb/10/electricity-market-operator-denies-being-asleep-at-the-wheel-during-blackout

Murphy, Z. (2011, 15 March). Japan earthquake: Living with blackouts. *BBC News*. https://www.bbc.com/news/world-asia-pacific-12731696.

Nakashima, E. (2011, 16 December). Foreign hackers targeted U.S. water plant in apparent malicious cyber-attack, expert says. *The Washington Post*, https://www.washingtonpost.com/blogs/checkpoint-washington/post/foreign-hackers-broke-into-illinois-water-plant-control-system-industry-expert-says/2011/11/18/gIQAgmTZYN_blog.html

National Health Executive (NHE) (2020, 12 October). WannaCry cyber-attack cost the NHS £92m after 19,000 appointments were cancelled". https://www.nationalhealthexecutive.com/News/wannacry-cyber-attack-cost-the-nhs-92m-after-19000-appointments-were-cancelled

Neal, Marian J. (2020, 16 December). COVID-19 and Water Resources Management: Reframing our priorities as a water sector." *Australian Aid*,

New Scientist (2000). Liquid petroleum gas explosion outside Sydney. https://www.newscientist.com/article/mg12617110-800-liquid-petroleum-gas-explosion-outside-sydney/

Office of Best Practice Regulation. (2020). Guidance Note: Small Business. Prime Minister and Cabinet. https://obpr.pmc.gov.au/sites/default/files/2021-06/small-business-guidance-note.pdf.

Oracle. What is a Domain Name System (DNS)?. https://www.oracle.com/au/cloud/networking/dns/what-is-dns/

Osbourne, C. (2018). NonPeyta ransomware forced Maersk to reinstall 4000 servers, 45000 PCs: The shipping giant has suffered millions of dollars in damage due to the ransomware attack. *ZDNet*, https://www.zdnet.com/article/maersk-forced-to-reinstall-4000-servers-45000-pcs-due-to-notpetya-attack/ 21 December

Palmer, D. (2017, 21 December). NotPeyta cyber-attack on TNT Express cost FedEx $300m. *ZDNe*t, https://www.zdnet.com/article/notpetya-cyber-attack-on-tnt-express-cost-fedex-300m/

Parliament of Australia. (2020). Security Legislation Amendment (Critical Infrastructure) Bill 2020. *Explanatory Memorandum*

Platonov V.; Semenov E.; Sokolikhina E. (2014). "Extreme La-Nina 2010/11 and the vigorous flood at the north-east of Australia". EGU General Assembly/Geophysical Research.

Pollard, E. (2021, 26 May). Queensland blackout to be investigated after fire at Callide Power Station cuts power to large parts of the state. *ABC News*, https://www.abc.net.au/news/2021-05-26/qld-callide-power-station-biloela-investigation/100164942.

The former Prime Minister of Australia. (2020, 19 June). Statement on malicious cyber activity against Australian networks. https://www.pm.gov.au/media/statement-malicious-cyber-activity-against-australian-networks

Queensland Floods Commission of Inquiry (2012). Final Report. http://www.floodcommission.qld.gov.au/__data/assets/pdf_file/0007/11698/QFCI-Final-Report-March-2012.pdf

Queensland Reconstruction Authority. (2011). The Community, Economic and Environmental Recovery and Reconstruction Implementation Plan 2011-2013. https://cabinet.qld.gov.au/documents/2011/apr/operation%20qlder%20implementation%20plan/Attachments/Implementation_Plan[1].pdf

Reserve Bank of Australia. (2018). Box D: Cyber Risk. Financial Stability Review.https://www.rba.gov.au/publications/fsr/2018/oct/box-d.html

Riley, D. (2021). Shipping company Forward Air discloses data theft following ransomware attack. *Silicon Angle*. https://siliconangle.com/2021/09/29/shipping-company-forward-air-discloses-data-theft-following-ransomware-attack/

Ritche, R. (2019). Maersk: Springing back from a catastrophic cyber-attack. *Global Intelligence for Digital Leaders*. https://www.i-cio.com/management/insight/item/maersk-springing-back-from-a-catastrophic-cyber-attack

Russon, M. (2021, 21 December). The cost of the Suez Canal Blockage. *BBC News*, https://www.bbc.com/news/business-56559073 21 December

San Jose Man Sentenced To Two Years Imprisonment For Damaging Cisco's Network. (2020). December 10. *United States Department of Justice*. https://www.justice.gov/usao-ndca/pr/san-jose-man-sentenced-two-years-imprisonment-damaging-cisco-s-network

Sayfayn, Nabil & Madnick, Stuart. (2017). Cybersafety Analysis of the Maroochy Shire Sewage Spill. *MIT Management Sloan School: Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity*, https://web.mit.edu/smadnick/www/wp/2017-09.pdf 14 December

SBS News. (2016, 9 December). SA blackout cost business $367 million. *SBS*. https://www.sbs.com.au/news/sa-blackout-cost-business-367-million,

Security Legislation Amendment (Critical Infrastructure) Act 2021 (Cth). https://www.legislation.gov.au/Details/C2021A00124

Shalvey, K. (2021, 21 December). Maersk, the world's largest shipping company, says the Suez Canal blockage's economic fallout will continue into second half of May. *Business Insider Australia*, https://www.businessinsider.com.au/maersk-ever-given-suez-canal-blockage-economic-fallout-late-may-2021-4

Smith, P. (2018). NAB's payments systems outage cost it millions in compensation. *Australian Financial Review.*

Smith, T. (2001, 16 December). Hacker jailed for revenge sewage attacks. *The Register*, https://www.theregister.com/2001/10/31/hacker_jailed_for_revenge_sewage/

South Australia Government. (2021). Frontier Software Data Breach. *South Australian Government*. https://www.sa.gov.au/topics/emergencies-and-safety/types/cyber-security/frontier-software-data-breach

Stracqualursi, V. Geneva, S. Saenz, A. (2021, 8 May). Cyberattack forces major US fuel pipeline to shut down. *CNN Politics*. https://edition.cnn.com/2021/05/08/politics/colonial-pipeline-cybersecurity-attack/index.html

Sutton, C. and Brown, N. (2020). Major roads closed due to horror fire conditions. *News.com.au*, https://www.news.com.au/technology/environment/major-roads-closed-due-to-horror-fire-conditions/news-story/bdfaaef1972b01584567bbb7549e0777

Swinhoe, D. (2019, 30 May). Why businesses don't report cybercrimes to law enforcement. *CSO Australia*. https://www.csoonline.com/article/3398700/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html.

Swinhoe, M. H. A. D. (2021). The 15 biggest data breaches of the 21st century. *CSO Online*. https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

Taylor, C. (2021). Empty shelves, gasoline shortages and sky-high energy process? Britain is facing a 'difficult winter'. *CNBC*. https://www.cnbc.com/2021/09/24/empty-shelves-and-gasoline-shortages-uk-facing-a-difficult-winter.html

Taylor, T. (2014). IT/OT Convergence. T&D World. https://www.tdworld.com/grid-innovations/article/20963808/itot-convergence.

TechCrunch is part of the Yahoo family of brands. (2019). *Tech Crunch*. https://techcrunch.com/2019/10/21/nordvpn-confirms-it-was-hacked/

The Australia and New Zealand School of Government. (2005, 14 December). The 1998 Sydney Water Crisis (A). https://www.anzsog.edu.au/preview-documents/case-study-level-1/127-1998-sydney-water-crisis-the-a-2005-22-1/file

The Maritime Executive. (2021). Ever Given's Owner Reaches Settlement with Suez Canal Authority. https://www.maritime-executive.com/article/ever-given-s-owner-reaches-settlement-with-suez-canal-authority 21 December

The National Aeronautics and Space Administration (NASA). (2018). What are radio waves?. *NASA* https://www.nasa.gov/directorates/heo/scan/communications/outreach/funfacts/what_are_radio_waves

The Office of Best Practice Regulation. "Securing Australia's Domestic Fuel Stocks and Refining Capacity". Department of Prime Minister and Cabinet. https://obpr.pmc.gov.au/published-impact-analyses-and-reports/securing-australias-domestic-fuel-stocks-and-refining

The Times of Israel. (2021). Iranian gas stations hit by outage in widespread cyberattack. https://www.timesofisrael.com/iranian-gas-stations-hit-by-outage-in-widespread-cyberattack/

The World Bank. (16 December) n.d. High and Dry: Climate Change, Water, and the Economy. https://www.worldbank.org/en/topic/water/publication/high-and-dry-climate-change-water-and-the-economy 16 December

Thomson, J. (2021). The hidden cost of your shutdown shopping spree. *Financial Review*, https://www.afr.com/companies/infrastructure/the-hidden-cost-of-our-covid-shopping-spree-20210120-p56vks

Turton, W. (2016). This is Why Half the Internet Shut Down Today. Gizmodo. https://gizmodo.com/this-is-probably-why-half-the-internet-shut-down-today-1788062835.

UNICEF. n.d. Water: Ensuring an adequate and safe water supply for the survival and growth of children. https://www.unicef.org/wash/water

United Nations. n.d. Water, Sanitation and Hygiene. UN Water. https://www.unwater.org/water-facts/water-sanitation-and-hygiene

United States Department of Justice. (2018, 10 August). Former JP Morgan Chase Bank Employee Sentenced to Four Years in Prison for Selling Customer Account Information. https://www.justice.gov/usao-edny/pr/former-jp-morgan-chase-bank-employee-sentenced-four-years-prison-selling-customer

United States Environmental Protection Agency. n.d. “Types of Drinking Water Contaminants.” https://www.epa.gov/ccl/types-drinking-water-contaminants#:~:text=Examples%20of%20chemical%20contaminants%20include,and%20human%20or%20animal%20drugs 16 December

UPI Archives. Liquid gas blast prompts mass evacuation in Sydney. https://www.upi.com/Archives/1990/04/01/Liquid-gas-blast-prompts-mass-evacuation-in-Sydney/9966638946000/

US - Canada Power System Outage Task Force. (2004). Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations. https://www3.epa.gov/region1/npdes/merrimackstation/pdfs/ar/AR-1165.pdf.

Victorian Auditor-General’s Office. (2020). Follow up of Managing the Level Crossing Program: Independent assurance report to parliament 2020-21:5. https://www.parliament.vic.gov.au/file_uploads/20201014-Follow-up_level_crossing_removal_report_k2c4ZRcV.pdf

Vision of Humanity. n.d. Global number of natural disasters increases ten times. https://www.visionofhumanity.org/global-number-of-natural-disasters-increases-ten-times/.

WaterAid Australia. (2016). Water and sanitation essential to fighting malnutrition. https://www.wateraid.org/au/articles/water-and-sanitation-essential-to-fighting-malnutrition 16 December

Whittaker, Z. (2021). A DNS outage just took down a large chunk of the internet. TechCrunch. https://techcrunch.com/2021/07/22/a-dns-outage-just-took-down-a-good-chunk-of-the-internet/

Williams, F. Robinson, C. (2021). Bilsdale transmitter fire: TV and radio for 1m off air indefinitely”. BBC News, 11 August. https://www.bbc.com/news/uk-england-tees-58169501

Wright, I. (2021). Victoria’s wild storms show how easily disasters can threaten our water supply. The Conversation, https://theconversation.com/victorias-wild-storms-show-how-easily-disasters-can-threaten-our-water-supply-162846

WWAP. (2016). The United Nations World Water Development Report 2016 Report: Water and Job; UNESCO

Yahoo News. (2011). Company: Cable cuts could slow Emirates Internet. https://web.archive.org/web/20160305035949/http://finance.yahoo.com/news/company-cable-cuts-could-slow-143049901.html

Zetter, Kim. (2011). H(ackers)2O: Attack on City Water Station Destroys Pump. Wired, https://www.wired.com/2011/11/hackers-destroy-water-pump/ 16 December

Appendix B: List of Acronyms

Acronym	Meaning
SLACIP Act	Security Legislation Amendment (Critical Infrastructure Protection) Act 2022
2020 RIS	Regulation Impact Statement: Critical Infrastructure, Systems of National Significance
ACSC	Australian Cyber Security Centre
ASA	Adverse Security Assessment
ASIO	Australian Security Intelligence Organisation
CIC	Critical Infrastructure Centre
CISC	Cyber and Infrastructure Security Centre
CISONS	Critical Infrastructure Systems of National Significance
CSIRO	Commonwealth Scientific and Industrial Research Organisation
FATA	*Foreign Acquisitions and Takeovers Act 1975* (Cth)
Government	The Commonwealth Government
IT	Information Technology
ISM	Australian Government Information Security Manual
ISO	International Organisation for Standardization
NDBS	Notifiable Data Breaches Scheme
OAIC	Office of the Australian Information Commissioner
PJCIS	Parliamentary Joint Committee on Intelligence and Security
RMP	Risk Management Program
RIS	Regulation Impact Statement
SOCI Act	*Security of Critical Infrastructure Act 2018* (Cth)
SLACI Act	*Security Legislation Amendment (Critical Infrastructure) Act 2021*
SLACI Bill	*Security Legislation Amendment (Critical Infrastructure) Bill 2020*
SLACIP	Security Legislation Amendment (Critical Infrastructure Protection)
The Department	The Department of Home Affairs
The Minister	The Minister for Home Affairs
TISN	Trusted Information Sharing Network

Appendix C: List of Tables and Figures

List of Tables

List of Figures

Appendix D: Draft General Rules

1. Responsible entities must, within six months of the commencement of this rule (or six months from first day of operation for new operators), ensure that their RMP includes a reasonable risk methodology.
2. Responsible entities must, within six months of the commencement of this rule (or six months from first day of operation for new operators), document in their RMP, the process by which the responsible entity has identified:
    a. What consideration they have given the elements of their business that are required to operate and support the daily functioning of the critical infrastructure asset; and
    b. the types of relevant impact that are most significant to the critical infrastructure asset; and
    c. any critical interdependencies with other critical infrastructure assets.
3. Responsible entities must, within six months of the commencement of this rule (or six months from first day of operation for new operators), ensure that their RMP includes details of the individual or individuals responsible for the development and implementation of the RMP as a whole, as well as the activities detailed within.
4. Responsible entities must, within six months of the commencement of this rule (or six months from first day of operation for new operators), document in their RMP how they will take a holistic approach to risk management, outlining how the entity will consider the relevant impact of different material risks on their assets and how the entity will implement appropriate mitigations to effectively minimise those threats or hazards across their organisation.
5. Responsible entities must, within six months of the commencement of this rule (or six months from first day of operation for new operators), ensure that their RMP outlines a process for regularly reviewing the RMP, including what circumstances would require a supplementary review.
6. Responsible entities must, within six months of the commencement of this rule (or six months from first day of operation for new operators), ensure that their RMP outlines a process for updating the RMP.

Appendix E: Draft RMP Rules

Note: Draft rules are structured by hazard vectors for the purposes of consultation, ease of discussion and costing. It is important to note that these are not the only hazards that responsible entities will need to consider in their risk management programs.

Timeframe	Risk management program requirements under the rules
Rules commence	Begin developing risk management program in line with Part 2A of the Act
	Begin identifying material risks, and thinking about the steps needed to minimise the risk of the hazards occurring, and mitigate the consequences should they occur (Material Risk Rules)
In six months	Have and comply with a risk management program in line with Part 2A of the Act
	Include the specified material risks, and take steps to minimise the risk of the hazards occurring and mitigate the consequences should they occur (Material Risk Rules)
	Ensure their risk management program includes details of a risk-based plan that outlines strategies and security controls as to how cyber and information security threats are being mitigated. (Cyber and Information Security Hazards Rule 1)
	Comply with all Personnel, Supply Chain, Physical and Natural Hazards rules.
Within 18 months	Ensure that their risk management program includes details of how the responsible entity complies with at least one of the following standards and frameworks: a) The Australian Cyber Security Centre's Essential Eight Maturity Model at maturity level one; b) AS ISO/IEC 27001:2015; c) The National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity; d) The Cybersecurity Capability Maturity Model (C2M2) at Maturity Indicator Level 1; e) Security Profile 1 of the Australian Energy Sector Cyber Security Framework; or f) an equivalent standard. (Cyber and Information Security Hazards Rule 2)

Obligations within the SLACIP Act which require responsible entities to comply with the risk management program rules once switched on will include a grace period of six months.

These draft rules are provided for the purpose of consultation and costing to inform advice to Government.

Material Risks

1. The SLACIP Act requires responsible entities to continue to identify and mitigate **material risks** that have a substantial impact the availability, reliability, and integrity of a critical infrastructure asset.
2. Responsible entities for critical infrastructure assets must consider **all** relevant **material risks** to their business.
3. Responsible entities for critical infrastructure assets are responsible for determining if a risk is a **material risk**.
4. Recognising the operating context differs between entities, when considering if a risk is a **material risk**, a risk management program should have regard to consideration of:
   a. a hazard that would cause the stoppage or major slowdown of a critical infrastructure asset's functioning for an unmanageable period;
   b. the substantive loss of access to or deliberate or accidental manipulation of a component of a critical infrastructure asset such as the position, navigation and timing systems impacting provision of service and/or functioning of the asset;
   c. the interference with a critical infrastructure asset's operating technology or information communication technology such as a Supervisory Control and Data Acquisition System (SCADA) system essential to the functioning of a critical infrastructure asset;
   d. the relevant impact on the critical infrastructure asset resulting from the storage, transmission or processing of sensitive operational information outside Australia;
   e. the relevant impact on the critical infrastructure asset resulting from the remote access to operational control or operational monitoring systems of the asset; and
   f. any other material risks as identified by the entity that go to the substance of the functioning of a critical infrastructure asset.

Rule 1 - Cyber and Information Security Hazards

1. Responsible entities for critical infrastructure assets **must**, within **6 months** of the commencement of this rule, ensure that their risk management program includes details of a risk-based plan that outlines strategies and security controls as to how cyber and information security threats are being mitigated.
2. Responsible entities for critical infrastructure assets **must**, within **18 months** of the commencement of this rule, ensure that their risk management program includes details of how the responsible entity complies with at least one of the following standards and frameworks:
   a. The Australian Cyber Security Centre's Essential Eight Maturity Model at maturity level one;
   b. AS ISO/IEC 27001:2015;
   c. The National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity;
   d. The Cybersecurity Capability Maturity Model (C2M2) at Maturity Indicator Level 1;
   e. Security Profile 1 of the Australian Energy Sector Cyber Security Framework; or
   f. an equivalent standard.

Rule 2 - Personnel Hazards

1. Responsible entities for critical infrastructure assets **must**, **within six months** of the commencement of this rule(or six months from first day of operation for new operators), ensure

that their risk management program includes details of how the entity identifies their critical positions and critical personnel[59] and includes a list of these positions and personnel, as appropriate.

2. Responsible entities for critical infrastructure assets **must**, within **six months** of the commencement of this rule (or six months from first day of operation for new operators), ensure that their risk management program includes details of how the entity ensures that the suitability of critical positions and critical personnel are appropriately managed, including but not limited to:
   a. assessing and managing the ongoing suitability of critical personnel and persons holding critical positions, through personnel and human resource arrangements; and
   b. considering, where commensurate with the risk environment, requiring an AusCheck or an equivalent vetting check for critical personnel.
3. Responsible entities for critical infrastructure assets **must**, within **six months** of the commencement of this rule (or six months from first day of operation for new operators), ensure that their risk management program includes details of how the entity mitigates risks arising from potential negligent personnel and malicious insiders who could cause damages to the functioning of a critical infrastructure asset.
4. Responsible entities for critical infrastructure assets **must**, within **six months** of the commencement of this rule (or six months from first day of operation for new operators), ensure that their risk management program includes details of how the entity manages risks arising from the off-boarding process for outgoing personnel.

Rule 3 - Supply Chain Hazards

1. Responsible entities for critical infrastructure assets **must**, within **six months** of the commencement of this rule (or six months from first day of operation for new operators), ensure that their risk management program includes details of strategies to secure the supply of products and services to critical assets to enable continued operation.
2. Responsible entities for critical infrastructure assets **must**, within **six months** of the commencement of this rule (or six months from first day of operation for new operators), ensure that their risk management program includes details of how the entity assesses and manages:
   a. unauthorised access, interference or exploitation of the critical infrastructure asset's supply chain;
   b. privileged access to the critical infrastructure asset by a provider(s) in the supply chain;
   c. disruption and sanctions of the critical infrastructure asset due to an issue in the supply chain;
   d. threats to people, assets, equipment, products, services, distribution and intellectual property within supply chains;
   e. vulnerability disclosure for other elements within supply chains;
   f. vendor dependency or reliance on entities inherently within supply chains.

---

[59] *Critical position* includes **but is not limited to**, a position in a responsible entity which has responsibility, access, control or management of the essential components or systems of the asset and where the absence or compromise of the position or its holder would prevent the proper function of the asset or could cause significant damage to the asset, as assessed by the responsible entity.

Critical personnel includes, **but is not limited to**, any employee of a responsible entity with responsibility, access, control or management of the essential components or systems of the asset and whose absence or compromise would prevent the proper function of the asset or could cause significant damage to the asset, as assessed by the responsible entity. The definition of personnel includes, but is not limited to, direct employees, interns, contractors and subcontractors.

Rule 4 - Physical and Natural Hazards

1. Responsible entities for critical infrastructure assets **must**, within **six months** of the commencement of this rule (or six months from first day of operation for new operators), ensure that their risk management program includes details of how the entity manages physical and natural hazards in their risk management program, at self-assessed critical sites.
2. Responsible entities for critical infrastructure assets **must**, within **six months** of the commencement of this rule (or six months from first day of operation for new operators), ensure that their risk management program includes details of how the entity seeks to minimise and mitigate the risk and relevant impacts of unauthorised access, interference and control of critical assets as well as the relevant impact of the natural hazards.
3. Responsible entities for critical infrastructure assets **must**, within **six months** of the commencement of this rule (or six months from first day of operation for new operators), ensure that their risk management program includes details of how the entity:
   a. Responds to incidents where unauthorised access occurs;
   b. controls authorised access, including restricting access to only those persons with the appropriate approval who have an operational need to access;
   c. conducts tests, as appropriate, to provide assurance that active security measures are effective and appropriate to detect, delay, and deter breaches of security; and gives consideration to how the responsible entity will respond and recover from breaches of security; and
   d. minimises, mitigates, and recovers from relevant impacts on their asset arising from natural hazards and disasters, including but not limited to bushfires, floods, cyclones, storms, heatwaves, earthquakes, tsunamis, health hazards such as pandemics.

Appendix F: List of consultation questions

Note: The consultation questions outlined below were used to incite discussion among workshop participants. These questions led to discussions and further questions from industry which may not be reflected in the table below.

Consultation phase	Topic	Question
Town hall	Critical infrastructure & systems of national significance reform	Has the information presented today helped address any concerns you may have had about being captured by the reforms? If you did have any concerns, what are they?
		Do you have any questions you would like to see addressed at the sector Q&A session?
	Rules (general)	Do you agree that the new approach to rules development will align with legislative intent? (uplift and assurance to government)
		Is there anything else you would like to comment on as we progress with sector engagement?
Information Session 1	CI / SONS reforms (general)	Are you clear on the intended approach?
		Are you confident that the explained process will achieve the intent of the legislation (resilience and security uplift of CI)?
		Do you have any further questions or comments?
		Has the information presented today allayed any concerns you may have about being captured by the reforms? If not, what additional concerns do you have?
	Consultation process (general)	Are there any specific questions you have in advance of further industry consultation around the costing process and the draft rules?
		Is there anything else you would like to comment on as we progress with sector engagement?
		What are we missing in these rules to make your sector safe?
		Do you have any questions or concerns about your feedback being heard?
	RMP rules (general)	Do the rules make sense?
		Are the rules implementable?
		Do you have any further questions or comments?
Information Session 2	RMP rules (general)	Are the RMP rules able to be implemented by your organisation?
		Do you feel informed on the RMP rules?
		Is there anything missing from the RMP rules necessary to keep your sector safe? If so, what?
		Which rules would benefit from additional guidance to assist with implementation of the rules?
		Are there any other questions or comments you're like to share with us?
	RIS	Is the RIS process clear and understandable?
		Is the timeline clear and understandable?
		Do you have you any other questions or comments?

Appendix G: Supplementary information for critical electricity assets

Overview of the role of electricity in Australia

The production, transmission, distribution, or supply of electricity is a major contributor to Australia's economy and is essential to efficiently conduct almost all day-to-day activities. As Australia's economy expands, the need for heightened security and resilience in Australia's critical electricity assets is increasing.

The lifecycle of electricity involves the following activities:

- **Generators** create electricity from various sources, including but not limited to coal, gas, solar, water, wind, and biomass.
- The electricity is then converted from low voltage to high voltage through **transmission networks**, which allow for greater efficiency in transporting electricity across long distances.
- Once the electricity is in close proximity to its geographical point of dissemination, **distribution networks** convert the high voltage electricity back to low voltage and transport the electricity to customers for use.

For 22 million Australians, electricity is provided by the National Electricity Market (NEM), covering the six eastern and southern states and territories. Western Australia and the Northern Territory manage their own electricity systems under separate regulatory arrangements.

The SOCI Act refers to assets within a critical infrastructure sector as 'critical infrastructure assets'. Section 10 of the SOCI Act outlines the following in relation to 'critical electricity assets' (underlined text is the proposed amendment):

*(1) An asset is a **critical electricity asset** if it is:*

(a) A network, system, or interconnector, for the transmission or distribution of electricity to ultimately service at least 100,000 customers or any other number of customers prescribed by the rules; or

(b) An electricity generation station that is critical to ensuring the security and reliability of electricity networks or electricity systems in a State or Territory, in accordance with subsection (2).

(2) *For the purposes of paragraph (1)(b), the rules may prescribe requirements for an electricity generation station to be critical to ensuring the security and reliability of electricity networks or electricity systems in a particular State or Territory.*

Impacts of a disruption to critical electricity asset

The consequences of a prolonged and widespread disruption to a critical electricity asset may include:

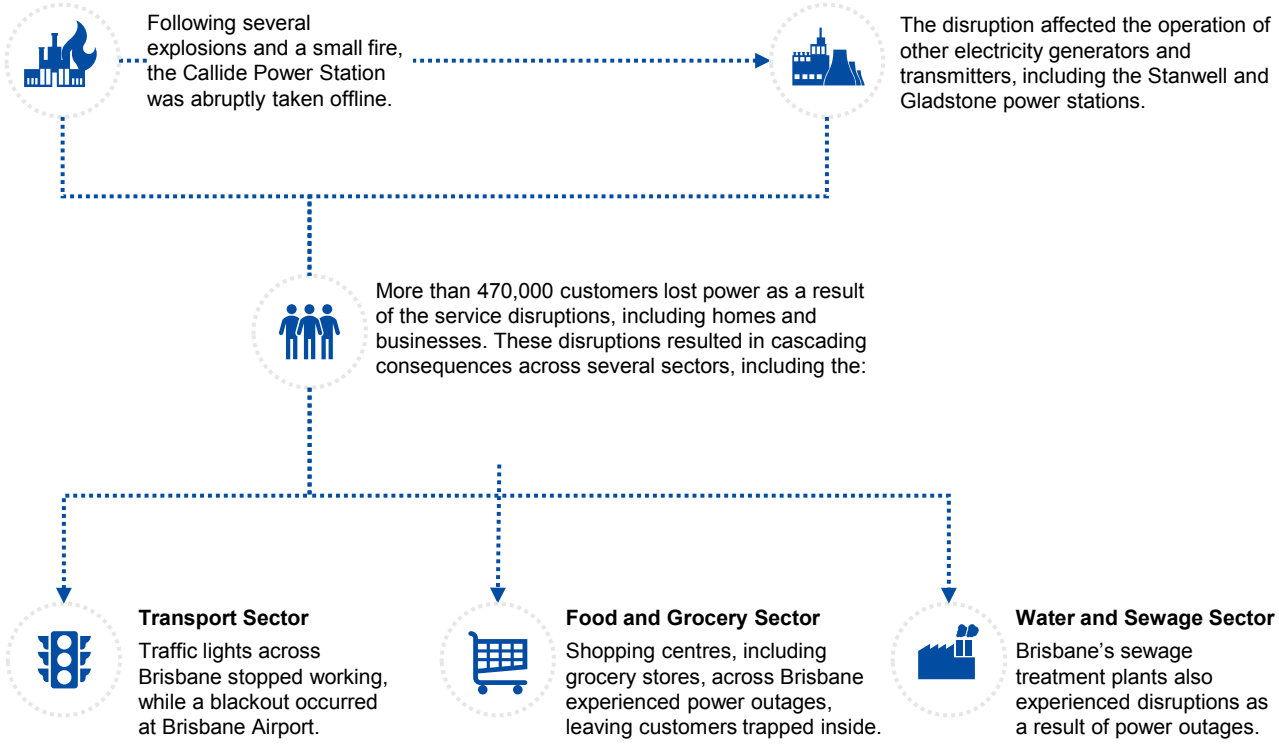
- shortages in or destruction of essential medical supplies which require refrigeration;
- reductions in the reliability of the supply of food and groceries;
- disruption to water supply and sanitation facilities;
- disruption to telecommunications networks which are dependent on electricity;
- disruptions to transport infrastructure, traffic management systems and fuel supplies;
- reduced services or closure of banking, finance and retail sectors;

- disruptions to Australia's defence capabilities;
- a reduction in social cohesion or public safety; and
- an inability for businesses and governments to function as normal.

Examples of disruptions to critical electricity assets – domestic and international

In May 2021, the Callide Power Station, located in Queensland was affected by an explosion which left more than 470,000 customers without power until it was restored with support from other states and with the help of renewables[60]. Damage to the power station itself was deemed 'catastrophic' and the incident had cascading effects for several other services across Queensland, as demonstrated by the figure below.[61] Following an inspection of the power station site, the original return to service dates of the three affected generators was delayed. While two affected units were deemed fit to return to service in June 2021, almost a month after the incident, the unit located at the explosion site will remain offline for a period of 12 months, as it must be entirely rebuilt.[62]

Cascading impacts of Callide power station explosion



Australia's summer bushfires threaten electricity grid (2020)	Natural hazard & physical risk

Situation: The Australian bushfires in the summer of 2020, which destroyed more than 10 million hectares of land and killed more than a billion animals, saw unprecedented pressure on Australia's electricity grid. While the biggest potential threat, that bushfires would strike the critical interconnector

[60] Pollard, 2021
[61] Rendall, 2021
[62] Ibid

linking the Victorian and New South Wales electricity grids, was not realised, accompanying extreme hot weather saw significant increases in the demand for electricity.[63]

Outcome: The combination of catastrophic bushfires and extreme weather conditions saw some Australian customers without electricity for an extended period of time. The Australian Energy Market Operator (AEMO) issued a level two 'lack of reserve' warning and signalled a potential need to call on emergency power reserves to avoid widespread blackouts. Approximately 10,000 customers in the Tumbarumba and South Coast regions, as well as an additional 5,800 were without electricity between New Years Eve of 2019 and early January 2020.[64]

Identified Gap: Rural towns and those residing on the edge of the electricity grid had no or insufficient back-up supplies or lacked a contingency plan. This caused power outages across regional communities and meant some critical electricity assets were unable to sustain operation for the duration of the bushfire disaster. The continued emergency reflected the need for smaller entities to have RMPs which reflect ways to mitigate the risks associated with the increase in natural hazards such as bushfires to prevent outages in the provision of electricity during times of emergency.

Ukraine's extended power disruptions (2015)	**Cyber & supply chain risk**

Situation: On 23 December 2015, malicious actors launched a sophisticated attack on the Ukrainian power grid, taking control of three energy distributors' Supervisory Control and Data Acquisition Networks. The attack saw the malicious actors attain remote access to and control over the firms' computers, allowing circuit breakers to be tripped and eventually taking thirty substations offline. Attackers also sought to disable or destroy other digital infrastructure, by wiping essential data from the companies' networks. Concurrently, a call centre that provided up to date information to consumers about the blackout was rendered inoperable due to a denial-of-service attack.

Outcome: While less than 1% of the country's daily consumption of energy was disrupted, the attack left over 225,000 Ukrainians, in the middle of winter, without power for several hours. Two months after the attack, some substations were still not fully operational and required manual operation to continue functioning.

Identified Gap: The attack is believed to be the first known cyber intrusion with success in downing the operation of a power grid. This incident highlights that while it is imperative to ensure the protection of critical electricity assets, supplementary and connected services must also be protected. For example, the disruption of the Ukraine power plant's customer service centre heightened, and prolonged, the effects of the attack itself.

[63] Foley, 2020

[64] Ibid

Malware attack on Saudi Arabian petrochemical plant (2017)	Physical, cyber & personnel risk

Situation: In 2017, hackers deployed malware on a Saudi Arabian petrochemical plant, which allowed remote access to and control over the plant's safety systems. The safety systems were designed as a 'last line of defence' against plant malfunctions, supporting plant processes in returning to safe levels or forcing them to cease operating where the threat of continued operation was too great.[1] The malware deployed to conduct the intrusion is widely suspected to be built by a nation-state actor.[65]

Outcome: A flaw in the hackers' code meant their infiltration operation was ultimately unsuccessful. However, had the hackers' infiltration been successful, it could have led to the release of toxic hydrogen sulphide gas or prompted explosions, putting at risk the lives of those who work at the facility and those in the surrounding area.[66]

Identified Gap: The attack highlighted the need for entities to maintain pace with evolving malware capabilities and work to strengthen their 'last line of defence'. Without adequate protections and consistent re-evaluations, operating systems considered critical to defending against catastrophic events, may be compromised.[67]

Japan's earthquake and tsunami cause blackouts (2011)	Supply chain & natural hazard risk

Situation: In March 2011, Japan experienced its strongest earthquake in history, which subsequently caused the Tohoku tsunami – producing waves of up to 40 meters. Following the disaster, large parts of Japan were plunged into darkness amid rolling blackouts caused from a drastic reduction in the supply of electricity. At the time of the incident, Japan relied on nuclear energy for approximately one quarter of its electricity. Of the country's 54 reactors, 11 were forced to close following the disaster, leaving 2.6 million households without power.[68]

Outcome: Environmental risks, such as natural disasters and weather events, are categorised as an external supply chain risk, with the Australian Productivity Commission recognising Japan's 2011 disaster as an example of an environmental hazard which caused significant disruption of supply chains.[69] Following the earthquake and tsunami:

- Electricity rationing was introduced, to account for the country's power shortfall;
- Utility companies were forced to approach their top commercial and industrial customers to request that they cut back on their energy usage;
- Train operations were decreased by 30-50% in order to save power; and

In the longer term, Japan began importing additional oil, fuel and natural gas resources, to account for the shortfall in electricity generation.[70]

Identified Gap: The Australian Productivity Commission suggests that the consequences of disruption, such as those caused in Japan, can be mitigated through increased preparedness. Japan's 2011 disaster was compounded by the nation's geographic clustering of key electricity-related infrastructure. Such clustering caused extensive market-level vulnerabilities, as many firms in the electricity industry were affected.[71] Diversified supply chains and advanced contingency planning can assist in reducing the levels of disruption caused by environmental risks.[72]

---

[65] Gonzalez, 2021
[66] Ibid
[67] Ibid
[68] Branigan, 2011
[69] Australian Government Productivity Commission, 2021
[70] Murphy, 2011
[71] Australian Government Productivity Commission, 2021
[72] Ibid

Key risks to critical electricity assets

Risk	Identified risk	Example
Physical	Increased occurrence of extreme weather events and natural disasters, including heatwaves, bushfires and floods, means physical electricity infrastructure is experiencing heightened pressure. This stems from both increased demand for energy and the threat or realisation of damage to critical infrastructure, such as power plants, power lines and pipelines.	In 2016, a series of severe thunderstorms triggered a state-wide blackout in South Australia. The incident damaged transmission and distribution assets and resulted in the suspension of the state's wholesale market for thirteen hours. The disruption is estimated to have cost South Australian businesses $120,000 per minute.[73]
	There is also a risk of sabotage by malicious actors to critical infrastructure's physical facilities. This could be used to disrupt the functioning of critical infrastructure and the systems which rely upon its function during times of heightened tension or conflict in the case of state-based actors.	In 1996 the Irish Republican Army (IRA) planned to disrupt the supply of electricity to the south east of England by destroying six electrical sub-stations with explosive devices. If the attack had been successful, there would have been a disruption in supply to the area for several months, with cascading disruptions across services reliant upon the electrical supply to function.[74]
Cyber	Electricity organisations have displayed greater reliance on software technology, to maintain pace with growing sector complexity and globalisation, creating the potential for unintended taint (where software design or implementation flaws increase susceptibility to cyber risks) and malicious taint (deliberate diversion or disruption to cyber supply chains intentionally introduces cyber risks).[75]	The AEMO has advised it is aware of sustained cyber-attack campaigns targeting Australia's electricity grid.[76] The AEMO advised that malicious actors such as the Avaddon Ransomware group had targeted more than 120 organisations globally, including critical infrastructure assets, with one Australian entity being attacked in early 2021.[77]
	Typically, electricity organisations have separated their Information Technology (IT) and Operational Technology (OT) systems. IT refers to software applications with capabilities in process management, resource allocation and decision-making, while OT allows for the operational control of assets within the network, in real time. The integration of OT and IT is desirable as the applications are able to work in tandem to optimise distribution system performance.[78] However, as this convergence occurs, many organisations are seeking to prioritise investment in IT security, while underestimating the significance of OT for completing critical business activities.[79]	Shodan, BinaryEdge, Censys and other similar search engines have created opportunities for malicious attacks on vulnerable OT and IT systems. Shodan, for example, allows users to search for, identify and access exposed devices, OT and IT systems, which are connected to the internet. The system provides user insights into the characteristics of listed devices and systems, expanding opportunities for exploitation (through, for example, defeating login safeguards). Where responsible entities have insufficient safeguards across their OT and IT systems, they may be vulnerable to physical breaches, unauthorised access to secure

[73] SBS News, 2016
[74] Bennetto, 1997
[75] Atlantic Counci,l 2018
[76] Australian Energy Market Operator, 2019; Australian Energy Market Operator, 2018
[77] Australian Energy Market Operator, 2021
[78] Taylor, 2014
[79] KPMG, 2020

Risk	Identified risk	Example
		information, and the destruction of data or essential services.[80]
Supply Chain	Disruption to supply chains pertinent to critical electricity assets may have detrimental consequences, as many project components and materials required for the maintenance of key pieces of electricity infrastructure are sourced from international suppliers.[81] This risk is compounded where organisations are primarily reliant on suppliers concentrated in a particular part of the world and may be concurrently affected by supply chain disruptions.[82]	The COVID-19 pandemic incited concern that the manufacturing and delivery of materials required for the maintenance of key pieces of electricity infrastructure be delayed, as required components must be sourced from Asia. Supply chain risks arose through the need for some electricity companies to cut back on capital and operational expenditures, which filtered down to suppliers and services companies who are reliant on upstream resources.[83]
Personnel	Where personnel are immobilised for reasons that cannot be controlled, critical electricity operations may be severely delayed or halted. Additionally, personnel with access to systems, data or premises may pose insider threat risks including fraud, theft, espionage, infrastructure sabotage and misuse of sensitive data.[84]	The COVID-19 pandemic saw key industry personnel subject to extended periods of quarantine, forcing the closure of some electricity generators or reduced capacity where insufficient personnel were available. Between 2013 and 2015, a series of attacks occurred on a company responsible for operating over 50 power plants across the US and Canada. The attacks were facilitated by information stolen by a company contractor and resulted in the theft of critical power plant designs and system passwords.[85]

[80] Ascierto, 2021
[81] Chenneveau, 2020
[82] Kilpatrick, 2021
[83] Deloitte, 2020
[84] Ernst & Young, 2016
[85] Johnston, 2017

Existing legislation related to electricity

Overview of regulation		Identified gaps
National Electricity (South Australia) Act 1996	Adopted as the model law, referred to as the National Electricity Law, and implemented (with minor amendments) across Australian State and Territory participants in the NEM. The equivalent State and Territory Acts include: • *Electricity (National Scheme) Act 1997* (ACT); • *National Electricity (New South Wales) Act 1997 No 20 & National Electricity (New South Wales) Law No 20a;* • *National Electricity (Northern Territory) (National Uniform Legislation) Act 2015;* • *Electricity – National Scheme (Queensland) Act 1997 & National Electricity (Queensland) Law;* • *Electricity – National Scheme (Tasmania) Act 1999 & National Electricity (Tasmania) Law;* and • *National Electricity (Victoria) Act 2005.* In Western Australia, the *Electricity Act 1945* and *Electricity Regulations 1947* operate, in addition to a series of other legislative frameworks. These schemes are similar in content and form to the National Electricity Law but operate as a separate regime.	The National Electricity Law is contained in a Schedule to the *National Electricity (South Australia) Act 1996* and seeks to establish the governance framework and key obligations for the NEM, including: • The functions of the AEMO; and • The regulation of access to electricity networks. The National Electricity Law is supported by the National Electricity Regulations and National Electricity Rules, which support the operation of the NEM. The National Electricity Law (and its subordinate legislation) does impose certain requirements on specific entities, with some implication for risk management. It requires the AEMO to maintain supply-demand balance (electrical supply security), but does not impose obligations around cyber, physical or other security. Furthermore, the National Electricity Law is primarily focussed on matters of governance and does not impose baseline risk reduction requirements on all entities. Finally, the National Electricity Law places obligations on AEMO to operate the system in a particular way, but does not apply obligations to each entity that operates a critical infrastructure asset.
Australian Energy Market Act 2004 (Cth)	Applies the National Electricity Law, the National Electricity Regulations and the National Electricity Rules as Commonwealth law in offshore areas as part of a uniform scheme of national electricity regulation.	This Act has, largely, an administrative function in applying the National Electricity Law in offshore areas. It does include provisions supplementary to the National Electricity Law and therefore, does not impose risk reduction requirements.
Electricity Supply (Safety and Network Management) Regulation 2014 (NSW)	These Regulations require that electricity network operators in New South Wales have in place a safety management system. Operators' systems are evaluated on an annual basis, with results published for public viewing.	While the mandatory requirement for a safety management system may contribute to suitable risk management, it does not amount to an all hazards approach to risk management, nor is the requirement for a safety management system imposed on a whole-of-sector basis.
Electricity Safety Act 1998 (VIC)	The Act mandates that major electricity companies in Victoria submit an electricity safety management scheme.	While the mandatory requirement for a safety management scheme may contribute to suitable risk management, it does not amount to an all hazards approach to risk management, nor is the requirement for a safety management scheme imposed on a whole-of-sector basis.

Overview of regulation		Identified gaps
State and Territory Emergency Management Legislation	Australia's States and Territories have in place emergency management legislation which may have a risk management element, including: • *Electricity Supply Act 1995* (NSW) • *Essential Goods and Services Act 1981* (NT) • *Electricity Reform Act 2000* (NT) • *Fuel Energy and Resources Act 1972* (WA) • *Essential Services Act 1981* (SA) • *Electricity Industry Act 2000* (VIC) • *Electricity Supply Industry Act 1995* (TAS) • *Utilities Act 2000* (ACT) • *Electricity Act 1994* (QLD)	While the risk management element contained in these legislative regimes may contribute to suitable risk management, they do not amount to an all hazards approach to risk management, nor are risk management obligations imposed on a whole-of-sector basis.
Electricity Supply Act 1995 (NSW)	Sets out the requirements relating to electricity suppliers. Under the Act, there are requirements to manage specific risks that may interrupt the supply of electricity. There is a section relating to emergency management with specific reference to bushfire prevention. There are some definitions relating to safety, accident reporting and investigation, and risk management. The Act includes regulation relating to the management of electricity supply emergencies, including the power for the Minister to give directions relating to the emergency. Has an energy security safeguard section which is designed to improve the affordability reliability and sustainability of energy through the creation of financial incentives.	While the Act has some risk management features in the sections relating to the management of electricity supply emergencies, and has requirements to reduce the risk of specific hazards such as bushfires, it does not amount to an all hazards approach to risk management. There is a lack of requirements to reduce cyber security, supply-chain and personnel hazards in the Act.
Independent Pricing and Regulatory Tribunal (IPART) Licence Conditions	IPART grants operating licences to four electricity network services in NSW (Ausgrid, Endeavour Energy, Essential Energy and TransGrid) under the *Electricity Supply Act 1995 (NSW)*. The licences include critical infrastructure conditions covering requirements for data security, ensuring a substantial presence in Australia. The licences include compliance obligations for reporting and independent auditing.	While there are some critical infrastructure security requirements in the operating licences, the licences do not require a holistic uplift of security. As such the licence conditions do not amount to an all hazards approach to risk management. The licences also only apply to electricity networks, and thus could not be used to regulate other energy assets/systems in NSW like electricity generators.

Note: The Department received feedback that some existing obligations were not reflected in the existing legislation. It is important to note that some jurisdictions have similar electricity provider obligations with regards to meeting supply standards/ensuring supply. While these obligations align with the purpose of the RMP, the Department does not consider them to be equivalent obligations. The requirement to ensure supply defines an outcome related to the service delivered. The RMP defines an outcome in relation to hazards that could affect the asset (which would affect the service delivered).

Existing standards, guidelines and regulators for critical electricity assets

Hazard domain	Organisation	Standards & guidelines
Cyber	AEMO Australian Cyber Security Centre (ACSC) Cyber and Infrastructure Security Centre Cyber Security Industry Working Group	**Australian Energy Sector Cyber Security Framework** (AESCSF) was developed with key industry and government stakeholders and leverages existing best practice standards for cyber security and safety, from Australia and overseas. The AESCSF incorporates the following Australian references: • ACSC Essential 8 Strategies to Mitigate Cyber Security Incidents; • The Australian Privacy Principles; and • The Notifiable Data Breaches Scheme.
	National Institutes of Standards and Technology (NIST)	**Cybersecurity Programs**
	International Organization for Standardization (ISO)	**ISO 27001** provides requirements for information security management systems.
	United States Department of Energy	**Cybersecurity Capability Maturity Model (C2M2)** was developed by the U.S. Department of Energy in conjunction with energy sector subject matter experts. It provides a voluntary evaluation process which allows entities to determine the maturity of their cyber security capabilities. The AESCSF is based upon this model.
	ACSC	**Essential Eight Maturity Model** provides requirements to increase business resilience against cyber and information security hazards.

Jurisdiction	Regulator/s
Commonwealth	Australian Energy Regulator (Responsible for regulating wholesale and retail energy markets and energy networks, under national energy legislation and rules. The AER sets network prices so that energy consumers pay no more than necessary for the safe and reliable delivery of electricity services, which includes setting the maximum amount of revenue which can be earned by electricity networks. The AER's regulatory functions relate, in particular, to energy markets in eastern and southern Australia.) Australian Energy Market Operator Energy Security Board (Provides whole of system oversight on energy security and reliability.)
Australian Capital Territory	Independent Competition and Regulatory Commission
New South Wales	Independent Pricing and Regulatory Tribunal of New South Wales
Northern Territory	Utilities Commission of the Northern Territory
Queensland	Department of Natural Resources, Mines and Energy
South Australia	Office of the Technical Regulator
Tasmania	Office of the Tasmanian Economic Regulator

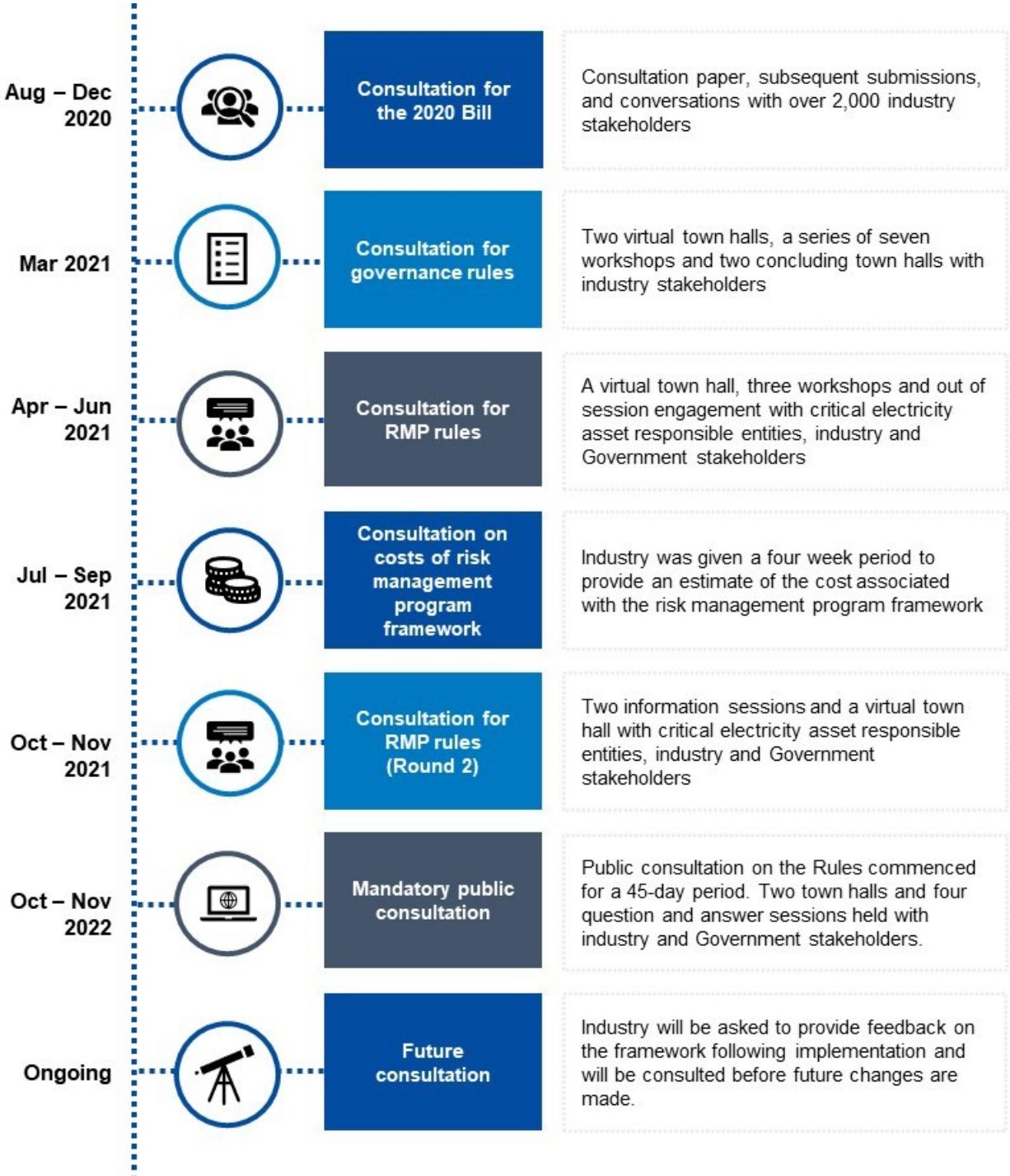
Victoria	Energy Safe Victoria
Western Australia	Economic Regulation Authority of Western Australia

Additional information on consultation

The table below contains an overview of the stakeholder organisations consulted.

Stakeholders Consulted	
• ActewAGL • AGL • AGL Energy Limited • Alinta Energy • ATCO • Ausgrid • AusNet Services • Australian Energy Council • Australian Energy Market Operator (AEMO) • Basslink • Caltex • Chamber of Minerals and Energy of Western Australian • CitiPower Powercor United Energy • Claroty • Clean Energy Council • Clean Energy Investor Group • CleanCo Qld • Clough • Delta Electricity • Diamond Offshore Drilling Inc. • ElectraNet • Endeavour Energy • Energy Australia • Energy Networks Australia • Energy Queensland Limited • Energy Users Association of Australia • Engie • Eni Australia Limited • Epic Energy • Equinor Asia Pacific Pty Ltd • Essential Energy • Evoenergy • GE • Hydro Tasmania • Incitec Pivot	• INPEX Australia • Jemena Energy • Kompression Communications • Kwinana Cogeneration Plant – IPM Operation & Maintenance • Loy Yang Power Station • Meridian Energy Australia • MODEC Management Services Pty Ltd • NRF • NRG GOS Power Gladstone • NT Power and Water • Oranj • Origin Energy • Pacific Hydro • Palisade Integrated Management Services Pty Ltd • Power and Water Corporation • PowerCor • Powerlink Queensland • SA Power Networks • Siemens Energy • Snowy Hydro Ltd • Stanwell Corporation • Synergy • TasNetworks • Telstra Energy • Thiess • Transgrid • United Energy • Vestas Wind Technologies • Viva Energy Australia Pty Ltd • WesCEF • Western Power • Wilson Transformer Co Pty Ltd • Worley

Consultation timeline



RMP Rules consultation

The Department undertook extensive consultation with the electricity industry for the design of the RMP Rules, with the objectives of:

- Assessing whether there are existing regulations that meet the SLACIP Act's RMP objectives, to ensure the regulatory burden is reduced where possible; and

- Ensuring there are rules in place that will drive an uplift in the security and resilience of critical electricity assets.[86]

Consultation with industry stakeholders occurred across the following key stages:

1. **A virtual town hall**, held in April 2021 attended by approximately 170 industry and Government stakeholders, to communicate the purpose of the co-design process and obtain information to inform the design of future workshops.
2. **A series of three virtual workshops**, held over a six-week period beginning in April 2021 and each attended by approximately 190 industry and Government stakeholders, which provided a forum to design RMP Rules and assisted in understanding the costs and benefits associated with implementing the risk management program framework. Workshops were designed to provide:
   i. Several opportunities for discussion and feedback to gather industry perspectives;
   ii. Polling, in-session surveys and facilitated discussions; and
   iii. 'Break out room' discussions, divided into generators, transmitters and distributors, to ensure comprehensive discussion occurred across all subsets of industry.
3. **Out of session consultation**, including meetings with a number of stakeholders and extensive email communication.
   – Stakeholders were encouraged to contact the Department out of session. The Department availed itself to stakeholders to discuss their concerns, working to ensure stakeholders' understanding of the rules, and the rules' proportionality.
   – Out of session engagement also assisted in the iterative development of rules between workshops, through addressing concerns raised by individual stakeholders and proposing a solution.
   – This engagement strengthened the relationship between the Department and industry, while providing insights on implementation costs, entities' operating environments and the overall impacts of the proposed regulatory changes.
4. **Two follow-up Consultation Sessions and two Industry-agnostic Town Halls** held in October and November 2021. The purpose of these consultation sessions was to provide an update for industry on the move from sector-specific to sector-agnostic RMP Rules and to gain sector-specific feedback on the updated RMP Rules. The purpose of the Industry Town Hall was to present the updated RMP Rules and provide information on the further consultation period. The two consultation sessions were attended by approximately 75 and 60 industry and Government stakeholders respectively. The two Town Halls were attended by approximately 800 industry and Government stakeholders across the 10 critical infrastructure sectors, including many stakeholders from the electricity sector.
5. **Mandatory Public Consultation**, following the Minister commencing a 45-day consultation period on 5 October 2022 (the mandatory period is 28 days). Consultation included two Town Hall Sessions held on 10 October and 12 October 2022, attended by approximately 550 industry and Government stakeholders (across both sessions). The sessions provided information on the proposed RMP Rules as well as the broader obligation. These Town Halls, as well as four subsequent question and answer sessions, provided an opportunity for industry to ask questions about the proposed RMP Rules and process.

[86] Department of Home Affairs, 2021, p. 2

Summary of Feedback from consultation sessions with responsible entities for critical electricity assets

Rule category	Identified themes		Impact on development of rules
Sector-agnostic RMP Rules	**Consultation Sessions**	• Industry believes the RMP Rules are **clear and understandable.** • Industry believes the RMP Rules will **be able to be implemented.** • The RMP Rules provide a **baseline** for sector resilience and security. • There is an **appetite for guidance material** to support sector-specific uplift in security and resilience.	In response to feedback received during the consultation sessions, the Department committed to: • The development of guidance materials, which would highlight aspects of risk management that should be prioritised by responsible entities and assist industry in interpreting and implementing the rules to achieve an uplift in security and resilience.

Consultation on costs

Throughout the workshop series commencing in April 2021, industry was invited to provide feedback that would assist the Department in understanding the potential costs associated with the proposed risk management program framework. Industry was informed that their insights would be used to assess the impact of the proposed reforms during the rules' development and support the drafting of this RIS and its cost benefit analysis.

During workshop 3, attendees were invited to participate in cost impact data collection through the completion of a cost impact template. This template was designed to collect substantive costing data to supplement the anecdotal costing discussions which had occurred throughout the workshop series. Industry was asked to provide:

- Their demographic information;
- Effort and cost estimates split by one-off and ongoing costs, staff effort, capital and other operating costs, and an estimated range between expected costs and highest possible costs; and
- Any comments on key boundaries, assumptions and cost drivers attached to the costing estimates provided.

Industry was provided with the template on 9 June 2021, with submissions open for a period of four weeks and closing on 7 July 2021. Following an analysis of the cost impact submissions, these outcomes were shared with industry for comment for a period of two weeks. Following receipt of completed cost impact submissions, the Department engaged in targeted conversations with a selection of industry stakeholders. These conversations were designed to give the Department a better understanding of the basis and scope of industry's cost submissions.

The absence of entities within the sector that meet the definition of a small business indicated that consultation with the Australian Small Business and Family Enterprise Ombudsman was not required to identify expected costs to small businesses in preparing this RIS.[87]

The Department confirmed with industry that no additional costings would be requested on the evolved RMP Rules, as they are either similar to the previously costed rules or a specific rule has been removed and the cost estimate for that rule could be excluded from the estimate of regulatory burden.

[87] Office of Best Regulation Practice, 2021

Consultation on draft RIS

A draft RIS was prepared using the costing information provided by industry. The draft RIS, accompanied by a feedback survey, was provided to industry on 6 August 2021. Industry was given two weeks to review and respond, with responses due back to the Department on 20 August 2021.

The Department received 14 responses to the feedback survey, from a range of generators, distributors and transmitters, as well Government departments. Overall, the survey responses demonstrated broad agreement with the consultation process and the recommended policy option. Where respondents indicated that particular elements of the RIS lacked clarity, the Department amended accordingly. Such amendments included:

- Additional rationale as to the chosen cost estimation methods;
- Clarification that indirect costs may be passed onto consumers (and that the economic impact of such costs are accounted for in CGE modelling approach);
- Additional rationale for selecting the South Australian blackouts as a baseline (moderate) risk scenario; and
- Reiteration of the Department's use of the 'on switch' mechanism to mitigate the potential for regulatory duplication.

The vast majority of comments in these submissions were regarding the draft sector-specific RMP Rules that the Department has subsequently moved away from. There were comments encouraging the Department to ensure that the final rules remain proportionate to the benefits, recommendations to extend the implementation timeline for particular rules, and comments on the potentially high cost of personnel rules. These concerns were considered in the shift to sector-agnostic rules through the following methods:

- Providing an 18-month period for industry to adhere to the standard based rule for cyber and information security hazards;
- Presenting AusCheck as an option for industry to use for personnel vetting without mandating its use
- The use of principles-based rules for most of the RMP rules to provide flexibility to industry in implementing the RMP obligation.

Appendix H: Supplementary information for critical gas assets

Overview of the role of gas in Australia

The production, processing, transmission, distribution, or supply of gas is a major contributor to Australia's economy and is essential to efficiently conduct almost all day-to-day activities. As Australia's economy expands, the need for heightened security and resilience in Australia's critical gas assets increases.

The lifecycle of gas involves:

- Sourcing gas from coal seam gas wells and offshore gas platforms, which involves drilling into coal seams and rock formations beneath the seabed to obtain a mixture of gas and liquid.
- Separation of the gas at a processing plant and then transmitted through high pressure pipelines to large industrial customers, LNG plants, electricity generators.
- Lowering gas pressure and sending to local distribution networks to be disseminated across residential areas or stored for distribution later.

Gas fields and pipelines in Australia are separated into three distinct gas regions: The East Coast which includes Queensland, New South Wales, the Australian Capital Territory, Victoria, Tasmania and South Australia; the Western region which includes Western Australia; and the northern region which includes the Northern Territory. All three regions sell gas to domestic and international customers. The East Coast gas region is an interconnected market with pipelines joining the five States and the ACT. The recently completed Northern Gas Pipeline has now also joined the Northern region to the East Coast market near Mount Isa. Some residential properties rely on safe and reliable gas supply for cooking, heating, and hot water. Approximately 20 per cent of Australia's electricity is generated by natural gas.

The SOCI Act refers to assets within a critical infrastructure sector as 'critical infrastructure assets'. Section 12 of the SOCI Act outlines the following in relation to 'critical gas assets':

*(3) An asset is a **critical gas asset** if it is:*

(c) a gas processing facility that has a capacity of at least 300 terajoules per day or any other capacity prescribed by the rules;

(d) a gas storage facility that has a maximum daily withdrawal capacity of at least 75 terajoules per day or any other maximum daily withdrawal capacity prescribed by the rules;

(e) a network or system for the distribution of gas to ultimately service at least 100,000 customers or any other number of customers prescribed by the rules;

(f) a gas transmission pipeline that is critical to ensuring the security and reliability of a gas market, in accordance with subsection (2).

Impacts of a disruption to critical gas assets

The consequences of a prolonged and widespread disruption to a critical gas asset may include:

- shortages or destruction of essential medical supplies which require refrigeration;
- unreliability in the supply of food and groceries;
- disruption to water supply and sanitation facilities;
- disruption to telecommunications networks which are ultimately dependent on gas;
- disruptions to transport infrastructure, traffic management systems and fuel supplies; and
- an inability for businesses and governments to function as normal.

Examples of disruptions to critical gas assets –domestic and international

Cyber Attack Shuts Down U.S. Fuel Pipeline System (2021)	Cyber & Supply Chain Risk
Situation: A cyber-attack allegedly conducted by a criminal network on the Colonial Pipeline, an 8,850km pipeline which carries almost half of the fuel consumed along the U.S. East Coast, forced the Pipeline's closure for almost a week. Although the infiltration immediately affected the Pipeline's business computer systems (rather than the systems which run the pipelines), the pipelines' closure was a necessary precaution while investigations were undertaken. The incident is thought to be the largest cyber-attack on oil infrastructure in the U.S.'s history.[88]	
Outcome: The pipelines' shutdown reduced the short-term availability of fuel, forcing fuel prices to climb and refiners to reduce production levels, as they had no means of distributing the gas. Consumers rushed to gas stations and engaged in 'panic buying', exacerbating shortages and contributing to price increases. In the first two hours following the attack, more than 100GB was stolen. On 13 May 2021, it was reported that Colonial Pipeline paid a ransom demand of close to $5 million USD in order to obtain a decryption key from the hackers responsible for the attack.[89] Chainalysis, a US cyber-security firm, suggests the amount paid in Bitcoin ransoms increased by 311% in 2020 (compared with 2019), to approximately $350m.[90]	
Identified Gap: The attack highlighted the need for entities to maintain pace with evolving malware capabilities and work to strengthen their 'last line of defence'. Without adequate protections and consistent re-evaluations, operating systems may be compromised.[91] It also highlights that while it is imperative to ensure the protection of critical gas assets, supplementary and connected services must also be preserved.	

Ransomware Attack on Mexico's Pemex (2019)	Cyber & Supply Chain Risk
Situation: In November 2019, a Mexican state-owned petroleum company was infiltrated by a ransomware attack, with attackers demanding approximately a USD $5 million ransom in bitcoin to remove the ransomware from the company's systems. Pemex was targeted by 'Ryuk', a kind of	

[88] Gonzalez, 2021
[89] Osborne, 2021
[90] The Economist, 2021
[91] Volz, 2018

ransomware which typically seeks to target companies with annual revenue between $500 million and $1 billion.[92]

Outcome: Hackers claimed the attack was successful in gathering sensitive data from the Pemex network and threatened to share the information publicly if the company did not pay the ransom. It is not clear whether Pemex paid the ransom amount. The attack allegedly impacted approximately 5% of the computers in Pemex's network, temporarily suspending staff access to computer systems, including those responsible for payments. Pemex became reliant on manual billing, which affected the payment of personnel, suppliers and hindered supply chain operations.[93] Staff were instructed to disconnect from its network and back up critical information from hard drives.

Identified Gap: The attack highlighted the need for entities to maintain pace with evolving malware capabilities, work to strengthen their data security initiatives and ensure adequate contingencies are in place in the event of an attack. This includes ensuring that protections and contingencies reach sufficiently far back in an entities' supply chain.

Varanus Island disruption, Western Australia (2008)	**Physical Risk**

Situation: In June 2008, a major disruption to the natural gas supply in Western Australia occurred after an explosion at the Apache Energy operated processing plant on Varanus Island, off the state's north west coast. The explosion and subsequent fire at the processing plant was caused as a result of a rupture of a corroded gas export pipeline. The main causal factors of the incident were ineffective anti-corrosion coating and cathodic protection on the gas pipeline and ineffective monitoring and inspection by Apache Energy.

Outcome: The explosion and subsequent fire caused widespread damage at the plant. Apache Energy's plant was immediately shut down, reducing Western Australia's gas supply by around 30% for over two months while a detailed engineering investigation and major repairs were carried out. Gas spot prices increased sharply, and several mining and industrial companies were forced to curtail production. Some electricity generators switched to emergency diesel stocks, and coal fired power plants that had been closed were also brought back online.[94]

Identified Gap: This incident demonstrates the importance of effectively maintaining all physical assets and having an appropriate framework in place for the monitoring and inspection of physical assets. This incident highlights the importance of having an effective Risk management Program implemented.

Enbridge Natural Gas Pipeline Explosion in Canada (2018)	**Physical, Supply Chain & Personnel Risk**

Situation: In 2018, undetected stress corrosion cracking saw the rupture of Canada's Enbridge pipeline, which resulted in a fire near the city of Prince George, British Columbia province. The pipes' external stress corrosion cracks had broken down over time and significantly reduced the pipeline's load-bearing capabilities. The Transportation Safety Board of Canada found that personnel and equipment deficiencies in detecting the extent of the cracking, as well as the deferral of a routine inspection, allowed the pipeline's

[92] Barrera, 2019

[93] Sussman, 2019

[94] Government of Western Australia – Office of Energy, 2009

vulnerabilities to go undetected. There were no records indicating that a proposed deviation, rationale or technical assessment had been completed, or that an inspection deferral request had been approved.[95]

Outcome: The rupture and subsequent fire caused significant damage to the pipeline and surrounding environment, compounded by substantial natural gas leakages from the pipeline. The rupture forced the evacuation of approximately 125 residents within a 2km radius of the explosion site, resulted in province-wide natural gas shortages and required heightened energy conservation efforts throughout winter. Despite this, emergency response activities were considered successful in mitigating the impacts of the incident.

Identified Gap: This incident demonstrates the importance of implementing incentives for risk management compliance, to reduce the potential that critical assessment, evaluation and reporting practices are not ignored or unnecessarily postponed. Without this incentive, entities may overlook deficiencies in their critical gas assets, compounding the risk and subsequent consequences of a potential disruption.

US natural gas compressor cyber-attack (2020)	**Cyber & Supply Chain Risk**

Situation: A major U.S. natural gas compression facility was entirely shut down for two days due to a ransomware attack. The attackers gained control of the facilities information technology system by through malicious links in phishing emails. The attacker deployed the commodity ransomware to encrypt data on both the operational and information technology networks at the same time before demanding a ransom payment.[96]

Outcome: According to a security alert issued by the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the ransomware attack led to the facility being shut down for two days. The shutdown led to a loss of productivity and decrease in revenue.

Identified Gap: The entity attacked had an insufficient cyber emergency response plan as their existing emergency response plan focused on threats to physical safety and not cyber incidents. The incident also highlighted an inadequate segregation of IT and OT systems and insufficient personnel training on cyber and phishing attacks.

Cyberattack on US shared data network (2018)	**Cyber & Supply Chain Risk**

Situation: In June 2018, a cyberattack on a shared data network forced four natural-gas pipeline operators in the U.S. to temporarily shut down computer communications with their customers. The attack's target appears to have been Latitude Technologies, a Texas-based provider of electronic data-sharing between pipeline companies and their gas producer and utility customers.

Outcome: The cyberattack led to a temporary shutdown in customer communications for the four operators. There was no impact to gas supply and no customer data was compromised. Although the incident did not affect any gas supplies, the attack shows the potential vulnerability of gas networks to cyberattacks and the significant impact that would occur.

Identified Gap: The cyberattack highlighted the need for entities to maintain pace with evolving malware capabilities, work to strengthen their data security initiatives and ensure adequate contingencies are in

[95] Transport Safety Board of Canada, 2018

[96] US Cybersecurity and Infrastructure Security Agency, 2020

place in the event of an attack.

Disruption to Longford gas plant (2021)	Physical & Supply Chain Risk
Situation: The Longford gas plant in Victoria, the largest domestic gas production plant on the east coast suffered a disruption to production due to technical problems over a weekend in mid-July 2021, triggering a spike in prices. Gas production at Longford fell due to reported issues with the gas dehydrators.	
Outcome: The decrease in gas supply meant that Victorian wholesale gas price jumped to $39.99 a gigajoule on Saturday afternoon, about six times the average earlier in the year. The plant's production was reduced by about 30-35% for more than 24 hours due to technical problems.[97]	
Identified Gap: The disruption highlighted the need for multiple supply sources and adequate contingencies in the event of an incident.	

[97] Australian Financial Review, *2020.*

Key risks to critical gas assets

Risk	Identified risk	Example
Physical	Increased occurrence of extreme weather events and natural disasters, including heatwaves, bushfires and floods, means physical gas infrastructure is experiencing heightened pressure. This stems from both increased demand for energy and the threat or realisation of damage to critical infrastructure, such as power plants, power lines and pipelines.	The Australian bushfires in the summer of 2020, which destroyed more than 10 million hectares of land and killed more than a billion animals, put unprecedented pressure on Australia's critical gas assets. The combination of catastrophic bushfires and extreme weather conditions saw some Australian customers without electricity for an extended period. The Australian Energy Market Operator (AEMO) issued a level two 'lack of reserve' warning and signalled a potential need to call on emergency power reserves to avoid widespread blackouts. Approximately 10,000 customers in the Tumbarumba and South Coast regions, as well as an additional 5,800 Australians, were without electricity between New Years Eve of 2019 and early January 2020.[98]
Cyber	Critical gas assets are vulnerable to potential cyber-attacks at the production, transportation and distribution stages. Due to constant improvements in infiltration capabilities, it has become easier to carry out destructive cyber-attacks that cause operational and environmental disruptions to critical gas assets.	In 2017, hackers deployed malware on a Saudi Arabian petrochemical plant, which allowed remote access to and control over the plant's safety systems. The safety systems were designed as a 'last line of defence' against plant malfunctions, supporting plant processes in returning to safe levels or forcing them to cease operating where the threat of continued operation was too great.[99] Had the hackers' infiltration been successful, it could have led to the release of toxic hydrogen sulphide gas or prompted explosions, putting at risk the lives of those who work at the facility and those in the surrounding area.[100]
Supply Chain	Critical gas assets rely heavily on international relationships, leaving, at times, suppliers and service providers vulnerable to the consequences of political instability and environmental concerns. Supply disruptions have the ability to immediately and detrimentally effect oil and gas prices.[101]	The COVID-19 pandemic resulted in a reduced need for gas products, stemming from industrial stoppages and travel restrictions. Supply chain risks arose through the need for some gas companies to cut back on capital and operational expenditures, which filtered down to suppliers and services companies who are reliant on upstream resources.[102]
Personnel	Where personnel are immobilised for reasons that cannot be controlled, critical gas operations may be severely delayed or halted.	The COVID-19 pandemic saw key industry personnel subject to extended periods of quarantine, forcing the closure of some gas generators or reduced capacity where insufficient personnel were available. Further, in the wake of extensive retrenchments to preserve and maintain economic viability through the pandemic, gas companies may face skilled labour shortages in the event of a market rebound.

[98] ABC, 2020

[99] Technology Review, 2019

[100] Ibid.

[101] Refinitiv, 2019

[102] Deloitte, 2020

Existing legislation related to critical gas assets

Overview of regulation		Identified gaps
National Gas (South Australia) Act 2008	Adopted as the model law, referred to as the National Gas Law, and implemented (with minor amendments) across Australian State and Territory participants in the National Gas Market. The equivalent State and Territory Acts include: • *National Gas (ACT) Act 2008;* • *National Gas (New South Wales) Act 2008 No 31 & National Gas (New South Wales) Law No 31a;* • *National Gas (Northern Territory) Act 2008;* • *National Gas (Queensland) Act 2008;* • *National Gas (Tasmania) Act 2008; and* • *National Gas (Victoria) Act 2008.* Western Australia participates in the National Gas Market to the extent set out in the *National Gas Access (WA) Act 2009*.	The National Gas Law is contained in a Schedule to the *National Gas (South Australia) Act 2008* and sets out a State and Territory access regime for gas pipelines, which are subject to either 'light' or 'full' regulation, if classified as 'covered' pipelines. A person seeking access to a natural gas pipeline must satisfy certain criteria before obtaining a statutory right of access.[103] The National Gas Law is supported by the National Gas Regulations and National Gas Rules, which govern access to natural gas pipeline services. However, the National Gas Law is focussed on access and licensing regimes. It does not impose baseline risk reduction requirements on entities.
Australian Energy Market Act 2004 (Cth)	Applies the National Gas Law, the National Gas Regulations and the National Gas Rules as Commonwealth law in offshore areas as part of a uniform scheme of national electricity regulation.	This Act has, largely, an administrative purpose in applying the National Gas Law in offshore areas. It does not seek to impose any provisions supplementary to the National Gas Law and therefore, does not impose risk reduction requirements.
Customs (Prohibited Exports) Regulations 1958 (Cth)	Division 6 of the Regulations introduces the Australian Domestic Gas Security Mechanism (ADGSM), designed to ensure a sufficient supply of natural gas is maintained to meet the Australia's needs. Where a supply shortfall arises, the ADGSM may mandate that Liquified Natural Gas projects limit their exports or find new gas sources.[104]	The ADGSM offers a targeted approach to securing Australia's supply chains only. It does not seek to mitigate threats which exist in other identified hazard domains – including physical, cyber and personnel risks.
Gas Supply Act 1996 (NSW) & Gas Supply (Safety and Network Management) Regulation 2013 (NSW)	Requires that all Network Operators in New South Wales submit a Safety and Operating Plan with the Secretary of the NSW Department of Planning & Environment.	While the requirement for a safety management system may contribute to suitable risk management, it does not amount to an all hazards approach to risk management, nor is the requirement for a Plan imposed on a whole-of-sector basis.

[103] Cunsolo n.d.

[104] Government n.d.

Overview of regulation		Identified gaps
Petroleum and Gas (Production and Safety) Act 2004 (QLD)	Requires that captured operators in Queensland have in place a safety management system which details, most relevantly, organisational safety policies, structures and responsibilities, a formal safety assessment including a systematic assessment of risks, how they may arise and how they will be controlled.	While the requirement for a safety management system may contribute to suitable risk management, it does not amount to an all hazards approach to risk management, nor is the requirement for a safety management system imposed on a whole-of-sector basis.
Gas Safety Act 1997 (VIC)	Imposes general duties on gas companies in Victoria, including a requirement to manage and operate facilities to minimise, as far as practicable, hazards and risks to the safety of the public and customers arising from gas, interruptions to the conveyance or supply of gas, and the reinstatement of an interrupted gas supply.	While a general duty to manage and operate gas facilities with hazards and risks in mind may contribute to suitable risk management, it does not amount to an all hazards approach to risk management, nor are the identified duties imposed on a whole-of-sector basis.

The National Gas Law, while providing a comprehensive framework for the operation and regulation of the NEM, does not offer guidelines for consistent risk management practice across all critical gas assets. While some states and territories have sought to supplement this national regime with other safety and risk management obligations, the interconnected nature of critical gas assets, and Australia's critical infrastructure as a whole (as discussed throughout this RIS) means consistent, national standards are imperative.

Existing standards, guidelines and regulators for critical gas assets

Hazard domain	Organisation	Standards & Guidelines
Cyber	AEMO Australian Cyber Security Centre (ACSC) Cyber Infrastructure and Security Centre Cyber Security Industry Working Group	**Australian Energy Sector Cyber Security Framework** (AESCSF) was developed with key industry and government stakeholders and leverages existing best practice standards for cyber security and safety, from Australia and overseas. The AESCSF incorporates the following Australian references: • ACSC Essential 8 Strategies to Mitigate Cyber Security Incidents; • The Australian Privacy Principles; and • The Notifiable Data Breaches Scheme.
	National Institutes of Standards and Technology (NIST)	**Cybersecurity Programs**
	International Organization for Standardization (ISO)	**ISO 27001** provides requirements for information security management systems. **ISO 27002** provides guidelines for organisational information security standards and security management practices.
	Australian Government	**Information Security Manual**
	International Electrotechnical Commission	**ISA/IEC 62443** standard specifies security capabilities for control system components. **ISO 31000** provides principles, a framework and a process for risk management.

Hazard domain	Organisation	Standards & Guidelines
Physical	Commonwealth Attorney-General's Department	**Protective Security Policy Framework** (PSPF) outlines the Government's protective security policy and ensures effective implementation by entities, in line with the following outcomes: • Security governance; • Information security; • Personnel security; and • Physical security.
	Energy Networks Association	**ENA DOC 015-2006** National Guidelines for Prevention of Unauthorised Access to Electricity Infrastructure.
	ISO	**ISO 55001** provides an overview of asset management.
	Australian Security Intelligence Organisation (ASIO)	**ASIO T4** Protective Security Advice for Australian Government Agencies.
Personnel	AEMO ACSC Cyber Infrastructure and Security Centre Cyber Security Industry Working Group	**AESCSF** Workforce Management Domain.
	Commonwealth Attorney-General's Department	**PSPF** (see above).
	ISO	**ISO 45001** provides the International Standard for health and safety management.
Supply Chain	AEMO ACSC Cyber Infrastructure and Security Centre Cyber Security Industry Working Group	**AESCSF** (see above).
	ISO	**ISO 22301** specifies requirements to implement, maintain and improve a management system to protect against, reduce the likelihood of the occurrence of, prepare for, respond to and recover from disruptions as they arise.

Jurisdiction	Regulator/s
Commonwealth	Australian Energy Regulator Australian Energy Market Operator Energy Security Board (Provides whole of system oversight on energy security and reliability)

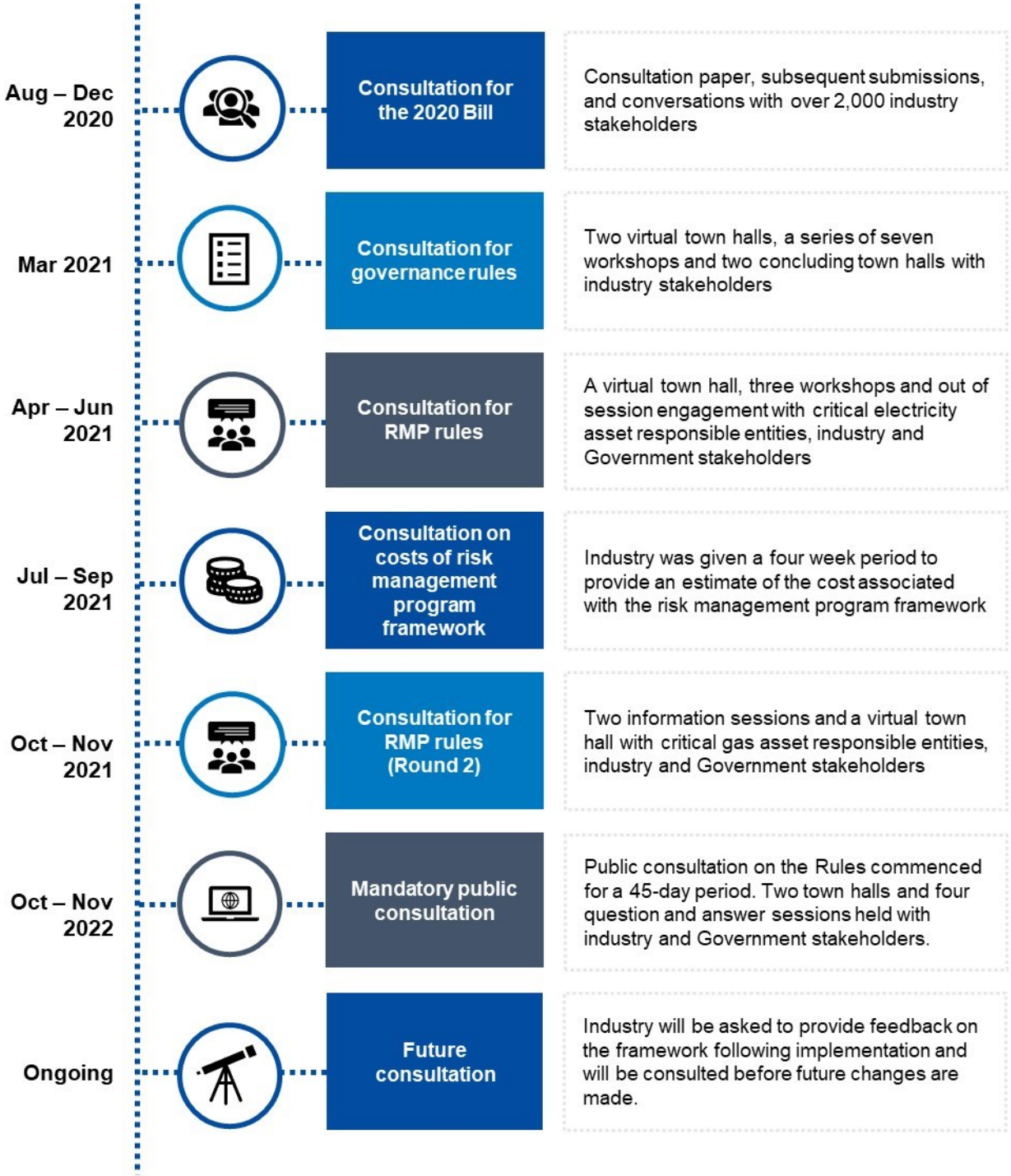
Australian Capital Territory	Independent Competition and Regulatory Commission
New South Wales	Independent Pricing and Regulatory Tribunal of New South Wales
Northern Territory	Utilities Commission of the Northern Territory
Queensland	Department of Natural Resources, Mines and Energy
South Australia	Office of the Technical Regulator
Tasmania	Office of the Tasmanian Economic Regulator
Victoria	Energy Safe Victoria
Western Australia	Economic Regulation Authority of Western Australia

Additional information on consultation

The table below contains an overview of the stakeholder organisations consulted during the consultation process.

Stakeholders Consulted	
• Australia New Zealand Industrial Gas Association • Australia Pacific LNG • Australia Pipelin and Gas Association • Australian Gas Infrastructure Group	• Conoco Philips Australia • Gas Energy Australia • GLNG Operations Pty Ltd • Lochard Energy • Santos LTD • Vermilion Oil and Gas Australia

Consultation timeline



RMP Rules consultation

Consultation with industry stakeholders occurred across the following key stages :

1. **A virtual town hall**, held on 28 April 2021 attended by approximately 79 industry and Government stakeholders, to communicate the purpose of the consultation process and obtain information to inform the design of future workshops.
2. **A series of three virtual workshops**, held over a six-week period beginning 11 May 2021 and each attended by approximately 50 industry and Government stakeholders, which provided a forum for the consultation of Risk Management Program rules and understand the costs and benefits associated with implementing the Risk Management Program Framework. Workshops were designed to provide:
   i. Several opportunities for discussion and feedback to gather industry perspectives;
   ii. Polling, in-session surveys and facilitated discussions; and
   iii. 'Break out room' discussions, divided into Generators, Transmitters and Distributors, to ensure comprehensive discussion occurred across all subsets of industry.
3. **Out of session consultation**, including meetings with a number of stakeholders and extensive email communication.
   – Stakeholders were encouraged to contact the Department out of session. The Department availed itself to stakeholders to discuss their concerns, working to ensure stakeholders' understanding of the rules, and the rules' proportionality.
   – Out of session engagement also assisted in the iterative development of rules between workshops, through addressing concerns raised by individual stakeholders and proposing a solution.
   – This engagement strengthened the relationship between the Department and industry, while providing insights on implementation costs, entities' operating environments and the overall impacts of the proposed regulatory changes.
4. **Two follow-up Information Sessions and one Industry-agnostic Town Hall** held in October and November 2021. The purpose of the information sessions was to provide an update for industry on the move from sector-specific to sector-agnostic Risk Management Program rules and to gain sector-specific feedback on the updated Risk Management Program rules. The purpose of the Industry Town Hall was to present the updated Risk Management Program rules and provide information on the further consultation period. The two information sessions were attended by approximately 160 and 200 industry and Government stakeholders respectively. The Town Hall was attended by approximately 800 industry and Government stakeholders across the 10 critical infrastructure sectors, including by many stakeholders from the gas sector.
5. **Mandatory Public Consultation**, following the Minister commencing a 45-day consultation period on 5 October 2022 (the mandatory period is 28 days). Consultation included two Town Hall Sessions held on 10 October and 12 October 2022, attended by approximately 550 industry and Government stakeholders (across both sessions). The sessions provided information on the proposed RMP Rules as well as the broader obligation. These Town Halls, as well as four subsequent question and answer sessions, provided an opportunity for industry to ask questions about the proposed RMP Rules and process.

Key themes from sector-specific consultation

Rule category	Identified themes		Impact on development of rules
Sector-agnostic Risk Management Program Rules	**Information Sessions**	• Industry believes the Risk Management Program Rules are **clear and understandable.** • Industry believes the Risk Management Program rules will **be able to be implemented.** • The Risk Management Program rules provide a **baseline** for sector resilience and security. • There is a **high appetite for guidance material** to support sector-specific uplift in security and resilience. • **Further clarity required** on material risk definitions – how to determine what may prejudice the 'social or economic stability', 'defence' or 'national security' of Australia.	In response to feedback received during the information sessions, the Department committed to: • The development of guidance materials, which would highlight aspects of risk management that should be prioritised by responsible entities, and assist industry in interpreting and implementing the rules to achieve an uplift in security and resilience.

Consultation on costs

During workshop 3, attendees were invited to participate in cost impact data collection through the completion of a cost impact template. This template was designed to collect substantive costing data to supplement the anecdotal costing discussions which had occurred throughout the workshop series. Industry were asked to provide:

- Their demographic information;
- Effort and cost estimates split by one-off and ongoing costs, staff effort, capital and other operating costs, and an estimated range between expected costs and highest possible costs; and
- Any comments on key boundaries, assumptions and cost drivers attached to the costing estimates provided.

Industry was provided with the template on 18 June 2021, with submissions open for a period of 13 weeks and closing on 18 September 2021. Following an analysis of the cost impact submissions, these outcomes were shared with industry for comment for a period of two weeks. Following receipt of completed cost impact submissions, the Department engaged in targeted conversations with a selection of industry stakeholders. These conversations assisted the Department in better understanding the basis and scope of industry's cost submissions.

The absence of entities within the sector that meet the definition of a small business indicated that consultation with the Australian Small Business and Family Enterprise Ombudsman was not required to identify expected costs to small businesses in preparing this RIS.[105]

The Department confirmed with industry that no additional costings would be requested on the evolved Risk Management Program rules, as they are either similar to the previously costed rules or a specific rule has been removed and the costings can be excluded.

[105] Office of Best Regulation Practice, 2021

Appendix I: Supplementary information for critical water assets

Overview of the role of water and sewerage in Australia

Australia's critical water assets, including critical sewage assets, are an essential part of life and critical for the ongoing health and prosperity of Australia. Critical water assets can be categorised into:

1. **Water supply assets**, including water catchment and bulk water supply services;
2. **Water distribution assets**, such as water reticulation systems; and
3. **Sewage and drainage services**, including water and sewage treatment plants and sewage network operations.

Following the accumulation, desalination, and initial treatment of water received in designated catchment facilities, water is ready for distribution and management through major water transmission piping. Further treatment is mandated for water used in industry and in particular, households, where vigorous drinking water standards are required to be met.

Critical water assets display diversity across both their geographical operations and interconnectedness with other aspects of Australia's critical infrastructure. For example, critical water assets are an essential input into Australia's energy sector, specifically in hydro-power generation, liquid and biofuel, and across fossil fuel power generation plants. These sectors display distinct co-dependence, with water required to generate electricity, and energy required to distribute water. Therefore, a disruption to critical water assets is likely to significantly disrupt the everyday lives of Australians.

The SOCI Act refers to assets within a critical infrastructure sector as 'critical infrastructure assets'. Section 5 of the SOCI Act provides that:

Critical water asset means one or more water and sewerage systems or networks that:

(a) are managed by a single water utility; and

(b) ultimately deliver services to at least 100,000 water connections or 100,000 sewerage connections.

Impacts of a disruption to critical water assets

The consequences of a prolonged and widespread disruption to a critical water asset may include:

- Heightened risk of illness and disease because of a lack of access to safe and clean drinking water, due to consuming water with chemical pollutants or other contaminants.[106]
- Additional burden on health systems including hospitals, with cleanliness and quality standards challenges through lack of access to clean water, sanitation or hygiene services.
- Economic instability and loss of productivity, with many energy sources and other industries dependent on the availability of water to function properly and without water, output may be severely restricted. Similarly, there is a direct impact on worker productivity when there is a lack of access to water, sanitation, and hygiene.[107]

[106] United States Environmental Protection Agency, n.d.; UNICEF, n.d.

[107] Arcadia, 2017

- Sanitation facilities become defunct:[108] when infrastructure cannot cope with increased demand or is deprived of necessary assets to function, which in this case is water, wastewater treatment systems and garbage and sanitation services cannot cope with the conditions that contribute to spread of disease and often results in water pooling.

Examples of disruptions to critical water assets – domestic and international

In 2020, one of Queensland's largest water entities, Sunwater (who is responsible for managing 19 dams and approximately 40% of Queensland's commercial-use water), was the victim of a cyber-attack which was continued for nine months. The cyber-attack was conducted by threat actors whose intentions to use IT infrastructure to direct bots to increase the amount of view on a particular YouTube video for financial gain.[1] The hackers were able to infiltrate an older and more vulnerable version of a Sunwater system. The hackers were able to operate within the system for nine months before the breach was identified[1]. The incident highlighted a significant threat opportunity in several areas:

- Financial and payment systems data could have been accessed for the company, potentially putting Sunwater and their partners at financial risk;
- Customer data could have been accessed, leaving thousands of customers at risk of financial loss, identity fraud and breach of confidential information;
- Should the threat attackers had more malicious intentions, they had opportunity to control operational systems, creating potential risks such as contamination of the Sunwater water supply, potentially exposing thousands to contaminated water which could cause sickness, severe illness, or possibly death.

Queensland Floods (2010-2011)	Physical and Natural Hazards
Situation: A series of natural disasters struck Queensland between November 2010 and February 2011, having catastrophic impacts across the entire state. Floods forced the evacuation of thousands of people, with at least 90 towns and 200,000 people affected.[109] The floods occurred in the wake of heavy rainfall caused by Tropical Cyclone Tasha that combined with a trough during the peak of a La Niña event.[110]	
Outcome: The floods saw three-quarters of the council areas within the state of Queensland declared disaster zones,[111] with communities along the Fitzroy, Burnett, Condamine, Ballone and Mary Rivers recording substantial flooding. Flash flooding caused by a thunderstorm affected Toowoomba, with the same rainfall hitting communities in the Lockyer Valley. Thousands of houses in Ipswich and Brisbane were inundated as the Brisbane River rose, caused by the forced release of water from the Wivenhoe Dam due to significant inflows.[112] 33 deaths were attributed to the floods.[113] Insurance claim payouts, Australian Government Disaster Recovery Payments, Disaster Income Recovery Subsidy payments, personal hardship and assistance payments, community wellbeing payments, grants, and other payments following the floods totalled $4.1 billion.[114]	
Identified Gap: This case study was not caused by the realisation of a specific threat, rather extreme compounding weather events which led to significant impacts on individuals, businesses, and the state as a whole. The case study does demonstrate the potentially catastrophic consequences of a compromise of critical water assets and the resulting impacts on lives and livelihoods. In an alternate scenario, the release of water from the Wivenhoe Dam (which was determined to be the primary cause of flooding of the Brisbane River) could be caused by compromise of the critical water asset as a result of an attack or other incident, with similar real-world impacts anticipated as what was experienced in 2011.	

[108] The Water Project, n.d.

Hackers Infiltrate and Modify Water Treatment Parameters	Physical and Cyber Hazards

Situation: In 2016, a company generically identified as Kemuri Water Company (KWC) noticed that its water treatment centre was operating erratically, with chemical values being modified without any manual intervention from company employees.[115] After its internal IT staff were unable to identify the issue, KWC enlisted the assistance from an external investigator who identified a series of issues, including that:

- KWC's computer systems were extremely outdated, some up to ten years old;
- The entire IT network was reliant on a single piece of equipment to manage the water treatment facility;
- The company's IT system was exposed to the internet, through an unsecure mechanism designed to allow customers to check their monthly water bills, water consumption levels and make bill payments; and

KWC had only one employee capable of managing its IT system, leaving the company vulnerable to cyber-attacks when that employee was off duty.[116]

Outcome: The external investigation determined that hackers were able to breach KWC's water treatment system through its customer payment application, allowing them to access sensitive personal and financial records for more than 2.5 million customers. The hackers then preceded to modify the chemical parameters of the water treatment plant at random. Ultimately, secondary security measures allowed KWC to detect abnormal chemical levels and adjust the parameters accordingly.[117]

Identified Gap: This case study demonstrates the need for critical water assets to ensure their computer systems are up to date, secure and that staff are adequately trained and knowledgeable on matters of cyber-security. It also emphasizes the importance of implementing secondary security systems, capable of detecting and mitigating threats which eventuate due to shortcomings in primary security mechanisms.

[109] BBC, 2010
[110] Platonov e. al, 2014
[111] Hurst, 2011
[112] Insurance Council of Australia, 2011
[113] Queensland Floods Commission of Inquiry, 2012
[114] Queensland Reconstruction Authority, 2011
[115] Softpedia News, 2016
[116] Ibid
[117] Ibid

Sydney Water Contamination Crisis (1998)	Physical Hazards

Situation: Between July and September 1998, microscopic pathogens cryptosporidium and giardia were detected in the water supply system of Greater Metropolitan Sydney. The detected levels were capable of causing stomach and diarrheal illness, with cryptosporidium capable of causing fatalities in people with weak immune systems.[118] The contamination was detected following routine water sampling and testing over a series of weeks, with the pathogens found in the drinking water of a number of Sydney suburbs and at several water treatment facilities. The affected suburbs received 'boil water' alerts and the NSW Health Department initiated enhanced surveillance, household surveys and increased water analysis to assure the quality of Sydney's water supply.[119]

Outcome: At the time of the incident, 3.5 million Sydney residents were told they may have to wait six months or longer before the quality of their water could be guaranteed.[120] The NSW Government established a Commission of Inquiry in response to the crisis, handing down a report which contained 91 recommendations, including the reorganisation of water supply, water management functions and agencies in Greater Metropolitan Sydney. While Sydney Water would maintain management of water supply distribution, water treatment and sewage, and stormwater management, the newly established Sydney Catchment Authority was allocated responsibility for catchments, dams and bulk supply reservoirs. Both the Chairman and Managing Director of Sydney Water stood down as a result of the crisis which was estimated to cost $33 million (in 1998).[121]

Identified Gap: This case study demonstrates the extent of the disruption which can be caused as a result of water quality issues. Water contamination can result in severe health and economic consequences for individuals, businesses reliant on water supply to support operations and, in this instance, costs associated with determining the cause of contamination and a plan for rectification. This case study highlights the need for Governments and private entities alike to have in place identification, mitigation and response mechanisms, in the event of water contamination incidents.

UK water supplier scammed through malicious insider (2017)	Cyber, Supply Chain & Personnel Hazards

Situation: Published in the 2017 Verizon Data Breach Digest Report, a UK water supplier discovered that the bank account details of several clients had been changed, and a total of £500,000 had been requested and sent to two bank accounts in England. Ninety percent of the funds were discovered to have been rewired to overseas accounts and then converted into Bitcoin. It was discovered that the source of the data breach was a call centre employee in Mumbai, working at the call centre to which the water supplier had outsourced its customer support operations. He had taken photos of the clients' CRM profiles and sent them to his cousin, who then initiated a reset password and changed the bank account details to his own account.

Outcome: With the help of a global law firm, the water supplier secured a conviction for the cousin, after having lost over $645,000 to the scam.

Identified Gap: This case study demonstrates how important it is for critical water assets to have risk management processes in place to protect sensitive data. It also demonstrates the need for critical water assets to be aware of and put in place practices to mitigate the effects of adverse action by employees, including ensuring through service level agreements that their critical vendors with access to sensitive data have commensurate personnel security policies.

Australian Man Perpetrates Revenge Sewage Attacks (2000)	Physical, Cyber & Personnel Hazards

Situation: Between March and April 2000, an Australian man conducted a series of 46 electronic attacks on the Maroochy Shire sewage control systems in the Maroochy Shire, Queensland. The attacks came after the man's job application was denied by the responsible Council. At the time of the attacks, the man was

[118] World Socialist Web Site, 1998

[119] The Australia and New Zealand School of Government, 2005

[120] Ibid

[121] Ibid

employed by the company who had installed the sewage control system. The man used his laptop, which contained software for accessing and controlling the sewage management system, to conduct the attacks.[122]

Outcome: The perpetrator of the attack was sentenced to two years imprisonment for infiltrating the Maroochy Shire's waste management system. The attack caused millions of litres of raw sewage to spill into local parks and rivers, including the ground of the Hyatt Regency Hotel. A representative from the Australian Environmental Protection Agency provided that, as a result of the attacks, '…marine life died, creek water turned black, and the stench was unbearable for residents.'[123] The incident cost the city council $176,000 in repairs, monitoring, clean-ups and extra security. Hunter Watertech spent more than $500,000 due to the incident.[124]

Identified Gap: This case study reiterates the need for critical water assets to have in place secure, up to date detection, protection and mitigation mechanisms to prevent the occurrence of attacks such as this. While this case study involves a prospective employee, rather than an ongoing employee, it also demonstrates the need for critical water assets to be aware of and put in place practices to mitigate the effects of adverse action by employees.

Attack on Illinois water station destroys pump (2011)	**Physical & Cyber Hazards**

Situation: In November 2011, it was reported that hackers had gained remote access into the control system of the city water utility in Springfield, Illinois, and destroyed a pump. The hackers were discovered on 8 November 2011, when an employee noticed problems in the city's Supervisory Control and Data Acquisition System (SCADA).[125] The system kept turning on and off, resulting in the burnout of a water pump. However, forensic evidence indicated that hackers may have infiltrated and remained in the system as early as September 2011. The intruders launched their attack from IP addresses based in Russia and gained access by first hacking into the network of a software vendor that makes the SCADA system. The hackers stole usernames and passwords that the vendor maintained for its customers, and then used those credentials to gain remote access to the utility's network.[126]

Outcome: This attack is one of the first of its kind, disrupting a system responsible for the supply of water, electricity and other essential services.[127] While past attacks have resulted in attempts to steal information or disrupt web services, this incident demonstrates the potential for cyber-attacks to cause physical disruption and destruction.[128]

Identified Gap: This case study demonstrates the potential vulnerability of critical water assets. For example, this incident raises the possibility that other customers using the vendor's SCADA system may be targeted as well. More broadly, it demonstrates the need for critical water assets to be aware of and put in place practices to mitigate the effects of potential cyber infiltrations.

[122] The Register, 2001
[123] Ibid
[124] Sayfayn & Madnick, 2017
[125] Wired, 2011
[126] Ibid.
[127] The Washington Post, 2011
[128] Ibid

Key risks to critical water assets

Hazard domain	Identified risk	Example
Physical Natural Hazard	An increase in extreme weather events across Australia and the world, including heatwaves, bushfires and flooding, can undermine the security of critical water assets by placing such assets under strain. Drought and subsequent flooding events also have the ability to create water scarcity events, or compromise the quality of drinking water, which can impact Australians' access to clean water.	In June 2021, extreme storm events across Victoria resulted in serious water contamination events. Yarra Valley Water issues an urgent health warning for three affected suburbs (Kalista, Sherbrook and The Patch) to refrain from drinking tap water, even if boiled. Yarra Valley Water provided that Victoria's severe weather events led to equipment failure, with potentially unsafe water entering the drinking water system.[129]
Cyber	As the complexity of critical water assets has developed, the risk of vulnerabilities rises, as many water utilities may not have been constructed with cyber security resilience in mind. This creates difficulties for detecting potential cyber infiltrations. The critical nature of water and dependent services means the mere detection of vulnerabilities can be problematic, as critical systems cannot be taken offline to undergo repair or upgrade. This reiterates the need for critical water assets to consider cyber security from the commencement of design, planning and operation.[130]	In June 2021, the United States' Water Information Sharing and Analysis Centre surveyed the water industry to determine entities' levels of cybersecurity preparedness. Specifically, more than 60% of water utilities say they have not fully identified IT-networked assets in their networks, and only a little more than 21% of those utilities said they are working to do so. Further, roughly 70% said they have not fully identified all OT (operational technology) networked assets and less than a quarter are working to do so.[131] In Australia, Auditor General audits have also highlighted cybersecurity deficiencies.
Supply Chain	A streamlined water supply chain and surety of water supply is imperative for the continued operation of critical water assets and other critical infrastructure assets. A suitable supply of water is essential to enable appropriate sanitation and hygiene practices. Where supply chains are undermined, as a result of disruptions to water treatment of distribution, essential services may be forced to cease operation. The price of water may be increased, placing a considerable burden on households and businesses. Further, where labour bases are interrupted, this can have a flow on affect to other services dependent on water – for example, food supply.[132]	The COVID-19 pandemic has reiterated the interconnections and interdependencies between water and essential services, across health, food, transport, environment and the economy. During the pandemic, many water utility providers were strained as a result of challenges to business continuity and risks arising across water supply and treatment chains and personnel availability (due to quarantine requirements). In a developing country context, these pressures were compounded by existing resource inadequacies, construction of eater treatment plants and inability to maintain existing water infrastructure.[133]

[129] The Conversation, 2021

[130] PSC Consulting, 2020

[131] GCN, 2021

[132] Australian Aid, 2020

[133] Ibid

Existing legislation related to critical water assets

Overview of regulation			Identified gaps
Commonwealth	*Criminal Code Act 1995*	Includes offences relating to: • computer intrusions; • unauthorised modification and destruction of data; • attacks on electronic communications; and • creation and distribution of malicious software. Dishonesty in obtaining or dealing in personal financial information. In 2018, the *National Security Legislation Amendment (Espionage and Foreign Interference) Act* amended the Criminal Code to broaden the range of espionage offences, including offences related to the sabotage of critical infrastructure and the theft of intellectual property.	This legislation applies penalties to individuals or groups who may seek to infiltrate critical infrastructure assets, rather than the operators of the assets. As such it does not enable a holistic uplift in the security of critical infrastructure in Australia.
	Water Efficiency Labelling & Standards Act	Aims to conserve water supplies through reducing water consumption, providing water use and water saving insights to consumers and promoting the adoption of efficient water conservation technologies.	This Act is primarily focussed on securing water supply. It does not address the safety and security threats which may undermine supply and therefore, does not encourage a holistic uplift in the security and resilience of critical water assets.
New South Wales	*Water Act 1912*	Sets out the obligations for water users in New South Wales, including licensing, permit requirements and joint water supply schemes. It provides for the state to create allocation schemes for water, and has some sections relating to environmental protection.	This Act is primarily focussed on the sustainable provision of water and the commercial behaviours of responsible entities. It does not address the safety and security threats which may undermine supply and therefor, does not encourage a holistic uplift in the security and resilience of critical water assets.
	Water Management Act 2000	This Act requires corporations to have measures in place to ensure the reliable supply of water and to have a water management plan. It includes some details on flood management for the Hunter Valley, partially addressing the Natural Hazard Vector.	While this Act refers to the protection of water resources, it does not discuss the security requirements defined in the *Australian Security Intelligence Organisation Act 1979*. It does not encourage a holistic uplift in the security and resilience of critical water assets.
Victoria	*Water Act 1989*	Sets out the requirements for sustainable water strategies, environmental water, water shares the allocation of water, water use licences, works, and permits. It also regulates water corporations, districts and land management areas, water supply and other matters related to water.	This Act is primarily focussed on water sustainability measures, rather than entities' risk practices. It does not address the safety and security threats which may undermine supply and therefor, does not encourage a holistic uplift in the security and resilience of critical water assets.

Overview of regulation			Identified gaps
	Safe Drinking Water 2003	Requires water suppliers to implement a risk management plan for water supplied for public consumption. This program must address any risks which may affect the quality of the water. It also stipulates drinking water quality standards and requires reporting on contaminated of water supply.	While this Act mandates the implementation of a RMP, such a program need not consider cyber, physical, supply chain, personnel or natural hazard risks. As such, it does not encourage a holistic uplift in the security and resilience of critical water assets.
Queensland	*Water Act 2000*	Outlined requirements for the supply of water during emergencies and the management and allocation of water across Queensland.	While these Acts offer some discussion on the processes surrounding water supply, they do not offer detailed requirements for risk management across all identified risk vectors. As such, they do not encourage a holistic uplift in the security and resilience of critical water assets.
	Water Supply (Safety and Reliability) Act 2008	Outlines the customer service, recycled water management, flood and drought mitigation standards for water service providers.	
South Australia	*Water Industry Act 2012*	Establishes, for the state's water sector, a licensing regime, pricing regulation, customer service standards, technical standards and performance monitoring processes. It empowers the Minister to impose additional requirements on responsible entities.	While this Act empowers the Minister to impose requirements on responsible entities in the listed categories, it does not address the security and resilience of critical water assets, across the identified risk vectors.
	Safe Drinking Water Act 2012	Requires risk management plans for the provision of safe drinking water, through identifying, assessing and managing the risks to water quality. The plans must also include monitoring, incident identification and notification protocol.	While this Act mandates the implementation of risk management plans, such plans need not consider cyber, physical, supply chain, personnel or natural hazard risks. As such, it does not encourage a holistic uplift in the security and resilience of critical water assets
WA	*Water Services Act 2012*	Sets out licencing arrangements for water services providers, compliance requirements and subsequent penalties for breaches of licensing arrangements.	The compliance measures outlined by this Act are not capable of uplifting the security and resilience of critical water assets.
Northern Territory	*Water Supply and Sewerage Services Act 2009*	Sets out requirements for entities responsible for the provision of water services, including criminalising interference with critical water infrastructure.	While this Act seeks to impose penalties for interference with critical water assets, it does not impose requirements for risk management practices to prevent the occurrence of such incidents. As such, it does not address the security and resilience of critical water assets, across the identified risk vectors.
	Waste Management and Pollution Control Act 1998	This piece of legislation imposes a burden to perform environmental duties, including notifying the Northern Territory Environmental Protection Agency of any incidents which cause or threaten to cause pollution.	While the requirement to notify may encourage responsible entities to manage the physical security of their hazards in terms of the requirement to manage potential hazards to water quality, it does not require entities to follow a RMP which identifies and manages all hazard vectors.

Overview of regulation			Identified gaps
Tasmania	*Water and Sewerage Industry Act 2008*	Defines the regulator and outlines requirements for licencing, customer service, price regulation, performance monitoring and the powers and obligations of regulated entities.	While this Act empowers the defined regulator to impose requirements on responsible entities in the listed categories, it does not address the security and resilience of critical water assets, across the identified risk vectors.
	Water Management Act 1999	Sets out the requirements for water management plans, water rights, the licencing and allocation of water and matters relating to water infrastructure, such as dams and meters.	This Act is primarily focussed on securing water supply. It does not address the safety and security threats which may undermine supply and therefor, does not encourage a holistic uplift in the security and resilience of critical water assets.
Australian Capital Territory	*Water Resources Act 2007*	Provides a framework for the protection of water resources, including provisions for water restrictions, licensing arrangements and management of unauthorised access to water resources.	This Act is primarily focussed on securing water supply. It does not address the safety and security threats which may undermine supply and therefor, does not encourage a holistic uplift in the security and resilience of critical water assets.
	Territory Owned Corporations Act 1990	Creates an audit committee with the ability to oversee the risk management practices of Territory-owned responsible water entities.	While this Act allows for the oversight of the risk management of some responsible entities, such powers do not apply to privately owned responsible entities. As such, it cannot incite an asset-wide uplift in security and resilience.

Existing standards, guidelines and regulators for critical water assets

Hazard domain	Organisation	Standards & guidelines
Cyber	International Organization for Standardization (ISO)	**ISO 27001** provides requirements for information security management systems.
Supply chain	Department of Climate Change, Energy, the Environment and Water	**Water Efficiency Program** increases water use efficient and recovers water for the environment. **Great Artesian Basin Strategic Management Plan** which regulates the amount of water that can be taken from the basin every year.
	Australian Government	**Inspector-General of Water Compliance** is a regulatory role to improve trust and transparency in implementing the Commonwealth's Basin water reform agenda delivering greater consistency and harmonisation of water regulation across the Basin and strengthen Basin Plan compliance and enforcement.
	National Water Quality Management Strategy: Australian Drinking Water Guidelines 6	The **Australian Drinking Water Guidelines (ADWG)** provides guidance to water regulators and suppliers on monitoring and managing drinking water quality. The ADWG provides details on the framework for Management of Drinking Water Quality (the Framework), a preventive management approach that encompasses all steps in water production from catchment to consumer, and aims to assure safe, good quality drinking water. The ADWG is used by state and territory health departments, local health authorities and water utilities.
	National Water Quality Management Strategy: Australian Drinking Water Guidelines 6	The Australian Drinking Water Guidelines (ADWG) provides guidance to water regulators and suppliers on monitoring and managing drinking water quality. The ADWG provides details on the framework for Management of Drinking Water Quality (the Framework), a preventative management approach that encompasses all steps in water production from catchment to consumer, and aims to assure safe, good quality drinking water. The ADWG is used by states and territories.
	National Water Quality Management Strategy	The National Water Quality Management Strategy (NWQMS) aims to assist water resource managers to understand and protect (which could be maintain or improve) water quality so that it is 'fit for purpose'— i.e., water that is suitable to desired values and uses and in accordance with specific local conditions. The NWQMS can also support the integration of water quality into water quantity planning.

Jurisdiction	Regulator/s
Commonwealth	• Attorney-General's Department • Australian Competition & Consumer Commission (ACCC) • Department of Climate Change, Energy, the Environment and Water • Department of Home Affairs • Murray-Darling Basin Authority • National Water Reform Committee (NWRC) • Water Quality Policy Sub Committee (WQPSC)
Australian Capital Territory	• Environment, Planning and Sustainable Development Directorate • Independent Competition and Regulatory Commission

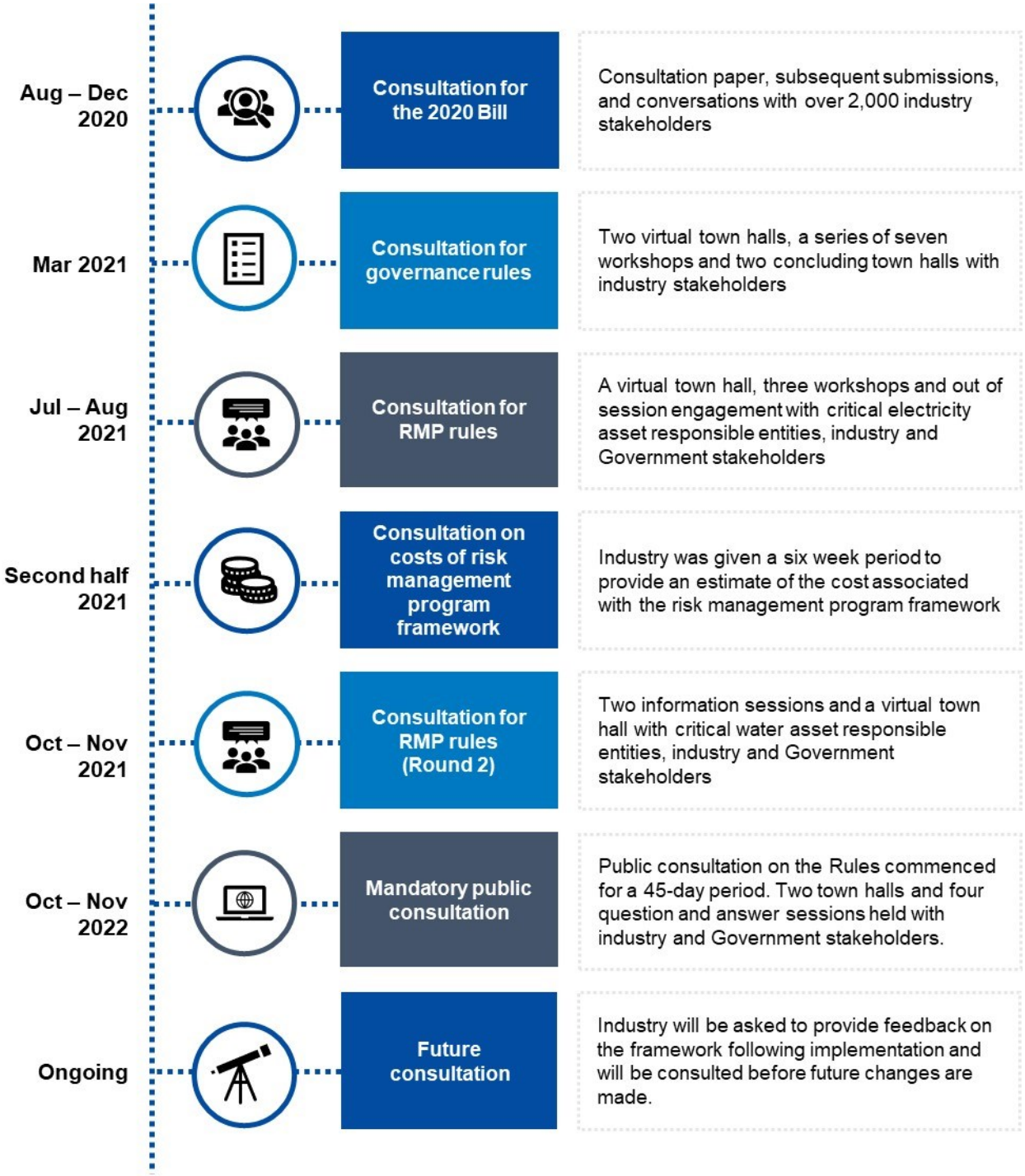
Jurisdiction	Regulator/s
New South Wales	• Department of Industry (DoI) Water (formerly DPI Water) • Independent Pricing and Regulatory Tribunal (IPART) • Natural Resources Access Regulator (NRAR) • New South Wales Department of Health • New South Wales Department of Planning, Industry & Environment • Water Infrastructure NSW
Northern Territory	• Northern Territory Government Department of Environment, Parks and Water Security • Power and Water • Utilities Commission of the Northern Territory
Queensland	• Department of Natural Resources, Mines and Energy (DNRME) • Director-General of the Department of Regional Development, Manufacturing and Water • Queensland Government Department of Environment and Science
South Australia	• Environment Protection Authority • Essential Services Commission of South Australia (ESCOSA) • Government of South Australia Department for Environment and Water • Government of South Australia Department of Treasury and Finance • Local Government Association of South Australia • SA Health • SA Water
Tasmania	• Environmental Protection Authority (EPA) Tasmania • Office of the Tasmanian Economic Regulator • Tasmanian Government Consumer, Building and Occupational Services • Tasmanian Government Department of Health • Tasmanian Government Department of Natural Resources and Environment Tasmania • Tasmanian Government Department of Treasury and Finance
Victoria	• Victorian Department of Environment, Land, Water & Planning (DELWP) • Environment Protection Authority (EPA) • Essential Services Commission • Victorian Catchment Management Council (VCMC)
Western Australia	• Economic Regulation Authority • Government of Western Australia Department of Health • Government of Western Australia Department of Water and Environmental Regulation

Additional information on consultation

Overview of stakeholders consulted

Stakeholders Consulted	
• Barwon Water • City of Gold Coast Water and Sewerage • Dams Safety NSW • Department of Regional Development, Manufacturing and Water • Economic Regulation Authority Western Australia • Greater Western Water • GWMWater • Hunter Water • Icon Water • Ixom • Mackay Regional Council • Melbourne Water • North East Water • Power Water	• South Australia Water • South East Water • Sunwater • Sydney Water • TasWater • The Water Directorate • Trility • Unity Water • Urban Utilities • VicWater • Water Corporation WA • Water NSW • Water Services Association of Australia (WSAA) • Yarra Valley Water

Consultation timeline



RMP Rules consultation

Consultation with industry stakeholders occurred across the following key stages:

1. **A virtual town hall**, held in July 2021 attended by approximately 83 industry and Government stakeholders, to communicate the purpose of the consultation process and obtain information to inform the design of future workshops.

2. **A series of 3 virtual workshops**, held over a six-week period beginning in July and August 2021 and each attended by approximately 90 industry and Government stakeholders, which provided a forum to consult on RMP Rules and assisted in understanding the costs and benefits associated with implementing the RMP framework. Workshops were designed to provide:

   i. Several opportunities for discussion and feedback to gather industry perspectives;

   ii. Polling, in-session surveys and facilitated discussions; and

   iii. 'Break out room' discussions, divided into [categories if applicable] to ensure comprehensive discussion occurred across all subsets of industry.

3. **Out-of-session consultation**, including meetings with several stakeholders and extensive email communication.

   – Stakeholders were encouraged to contact the Department out-of-session. The Department availed itself to stakeholders to discuss their concerns, working to ensure stakeholders' understanding of the rules, and the rules' proportionality.

   – Out-of-session engagement also assisted in the iterative development of rules between workshops, through addressing concerns raised by individual stakeholders and proposing a solution.

   – This engagement strengthened the relationship between the Department and industry, while providing insights on implementation costs, entities' operating environments and the overall impacts of the proposed regulatory changes.

4. **Two follow-up Consultation Sessions and two Industry-agnostic Town Halls** held in October and November 2021. The purpose of the consultation sessions was to provide an update for industry on the move from sector-specific to sector-agnostic RMP rules and to gain sector-specific feedback on the updated RMP rules. The purpose of the Industry Town Hall was to present the updated RMP rules and provide information on the further consultation period. The two consultation sessions were attended by approximately 75 and 60 industry and Government stakeholders respectively. The later Town Hall was attended by approximately 800 industry and Government stakeholders across the 10 critical infrastructure sectors, including by many stakeholders from the water and sewerage sector.

5. **Mandatory Public Consultation**, following the Minister commencing a 45-day consultation period on 5 October 2022 (the mandatory period is 28 days). Consultation included two Town Hall Sessions held on 10 October and 12 October 2022, attended by approximately 550 industry and Government stakeholders (across both sessions). The sessions provided information on the proposed RMP Rules as well as the broader obligation. These Town Halls, as well as four subsequent question and answer sessions, provided an opportunity for industry to ask questions about the proposed RMP Rules and process.

There were some concerns that the sector-agnostic rules would not provide enough sector-specific guidance on risk management processes to achieve an uplift in security and resilience. There were also concerns that the drafting of the sector-agnostic rules had not adequately leveraged the sector-specific discussions to-date. However, industry was appreciative of the Government's commitment to working with industry to provide sector-specific guidance material, which would be

both reflective of the sector's maturity levels and best practices, and easily updatable in response to new threats, to support a sustainable uplift in risk management practices. They understood that this guidance material would heavily leverage the sector-specific discussions to-date.

Key themes from consultation

Rule category	Identified themes		Impact on development of rules
Sector-agnostic RMP Rules	Information Sessions	• Industry mostly believes the RMP Rules are **clear and understandable.** • There is an **appetite for guidance material** to support sector-specific uplift in security and resilience and leverage sector-specific discussions to-date, particularly in designating appropriate equivalent standards. • There was a desire to move towards the previously agreed definition of '**critical positions'** rather than 'critical employees'.	In response to feedback received during the information sessions, the Department committed to: • The development of guidance materials, which would highlight aspects of risk management that should be prioritised by responsible entities and assist industry in interpreting and implementing the rules for their sector to achieve an uplift in security and resilience. • Changing the personnel hazards rules to refer to 'critical positions and/or critical personnel' rather than critical employees.

Consultation on costs

During workshop 3, attendees were invited to participate in cost impact data collection through the completion of a cost impact template. This template was designed to collect substantive costing data to supplement the anecdotal costing discussions which had occurred throughout the workshop series. Industry were asked to provide:

- Their demographic information;
- Effort and cost estimates split by one-off and ongoing costs, staff effort, capital and other operating costs, and an estimated range between expected costs and highest possible costs; and
- Any comments on key boundaries, assumptions and cost drivers attached to the costing estimates provided.

Industry was provided with the template on 12 November 2021, with submissions open for a period of four weeks and closing on 10 December 2021.

The absence of entities within the sector that meet the definition of a small business indicated that consultation with the Australian Small Business and Family Enterprise Ombudsman was not required to identify expected costs to small businesses in preparing this RIS.[134]

[134] Office of Best Regulation Practice, 2021

Appendix J: Supplementary information for critical data processing or storage assets

Overview of the role of data processing and storage in Australia

Data is an integral part of everyday life and commonly used by individuals, industry and governments across Australia. Data storage and processing is integral for the functioning of internet services, other digital services, the processing of payments, and the use of digital applications. The increasingly digital nature of Australian businesses and governments means the ongoing security and resilience of data storage and processing assets is critical and will become more important over time.

The table below provides an overview of Australia's critical data storage and processing assets, which can be categorised into:

1. Software-as-a-service (SaaS);
2. Infrastructure-as-a-service (IaaS); and
3. Platform-as-a-service (PaaS).

	On-premise Solutions	Models of Cloud Services		
		SaaS	IaaS	PaaS
Overview	Resources deployed 'in-house' and forming part of a business' IT infrastructure.	Also known as 'Cloud Application Services'. Leverages the Internet to deliver applications to its users, typically managed by third-party vendors. Represents the most common model for businesses in the cloud market.	Also known as 'Cloud Infrastructure Services'. Self-service model for monitoring computers, networking, storage and other services.	Also known as 'Cloud Platform Services'. Delivers a framework for user to build on and create customised applications.
Examples	Microsoft Office SAP Software & Solutions	Google Workspace Cisco WebEx	DigitalOcean Amazon Web Services	Force.com OpenShift

The SOCI Act refers to assets within a critical infrastructure sector as 'critical infrastructure assets'. The SOCI Act designates 'critical data storage and processing assets' as critical infrastructure assets and provides the following in relation to its definition:

*(1) An asset is a **critical data storage or processing** asset if:*

(a) it is owned or operated by an entity that is a data storage or processing provider; and

(b) it is used wholly or primarily to provide a data storage or processing service that is provided by the entity on a commercial basis to an end-user that is:

(i) the Commonwealth; or

(ii) a body corporate established by a law of the Commonwealth; or

(iii) a State; or

(iv) a body corporate established by a law of a State; or

(v) a Territory; or

(vi) a body corporate established by a law of a Territory; and

(c) the entity knows that the asset is used as described in paragraph (b).

(2) An asset is a critical data storage or processing asset if:

(a) it is owned or operated by an entity that is a data storage or processing provider; and

(b) it is used wholly or primarily to provide a data storage or processing service that:

(i) is provided by the entity on a commercial basis to an end-user that is the responsible entity for a critical infrastructure asset; and

(ii) relates to business critical data; and

(c) the entity knows that the asset is used as described in paragraph (b).

For the purposes of the SOCI Act, A **data storage or processing service** means:

(a) a service that enables end-users to store or back-up data; or

(b) a data processing service.

Meanwhile, the data storage or processing sector means the sector of the Australian economy that involves providing data storage or processing services.

Impacts of a disruption to critical data processing or storage assets

Data processing and storage assets are critical enabling function to a range of critical services across the economy. The consequences of a prolonged and widespread disruption to a critical data storage and processing asset may include:

- *Operational downtime* – business operations across the economy can be affected by the disruption of a critical data storage or processing asset. For example, point of sale (POS) technology may be disrupted resulting in an inability to purchase groceries or essential services.
- *Financial loss* – prolonged disruptions to data storage or processing assets supporting banking, financial and retail sectors may result in decreased business confidence and market contractions. Responsible entities may also be liable to compensate affected individuals or businesses for any damages because of disruptions.
- *Reputational damage* – reputational damage because of a data breach or disruption to data processing or storage asset can be severe. A loss of consumer trust in critical infrastructure, whether a specific entity or multiple, and subsequent behaviour can have flow-on implications such as increasing reliance on one or a smaller group of critical infrastructure entities.
- *Sensitive data loss* – any compromise of sensitive data (personal or other) can have significant impacts. For example, a disruption to a critical data storage or processing asset supporting the health sector could result in the theft or compromise of health information.

Examples of disruptions to critical data processing or storage assets – domestic and international

In November 2021, Frontier Software, one of Australia's largest software providers of payroll and HR services, was affected by a ransomware attack that left 330 employers without automated payroll for four days, as the company was forced to take down its server following the encryption of its systems.[135] This had cascading effects onto its customers, predominantly in healthcare, hospitality, Government and non-for-profit sectors, as they were forced to either delay pay runs or process them manually.[136] The ransomware attack also resulted in a data breach affecting at least 38,000 South Australian Government employees, with a number of employee's personal details being published on the dark web.[137]

Other case studies of incidents are included below.

Ransomware attack on IT services company Kaseya	Physical & Cyber Risk
Situation: In July 2017, hackers demanded USD70 million (AUD92.9 million) in bitcoin in exchange for data stolen during an attack on IT services company Kaseya.[138] Kaseya provides IT services to over 40,000 business globally, with the attack estimated to have affected more than 1,000 of these. Due to the nature of Kaseya's customer base, with some businesses retailing IT services underpinned by Kaseya's service offering, arrange of businesses were indirectly affected by the attack. Sweden's Coop supermarket chain was one of the indirectly affected entities, when its IT subcontractor Visma Esscom was hit by the attack.	
Outcome: Cybersecurity firm ESET identified victims in at least 17 countries, including South Africa, Britain, Mexico and Sweden. A range of essential services were affected – Coop's 800 supermarkets remained closed on the Monday after Friday's attack, with point-of-sale systems still affected and unable to operate. The attack was likely carried out by REvil, a Russian-speaking hacking group known for their frequent ransomware attacks. The hacker's blog post claiming responsibility for the attack also stated a decryption tool would be released once the bitcoin ransom had been paid. The hackers also reached out to demand smaller payments from individual affected companies, with reports of demands ranging from USD50,000 to USD5 million.	
Identified Gap: The Kaseya attack demonstrates the potential flow-on consequences as a result of compromise of key cogs in the data processing or storage sector, as well as the importance of understanding potential vulnerabilities underpinning critical infrastructure providing by third parties. While there is uncertainty over the specific payments made as a result of the attack, the amount demanded demonstrates the potentially extreme financial implications of ransomware attacks in addition to the financial impacts of reduced or impacted operations of essential services.	

Record-Breaking Google Cloud distributed denial of service (DDoS) Attack (2017)	**Physical & Cyber Risk**
Situation: In September 2017, Google experienced its largest recorded DDoS attack. The attack was not publicly disclosed until October 2020. The attack was alleged to have originated in China, from within a network of four Chinese internet service providers. A Security Reliability Engineer for Google Cloud said the attack represented "…the culmination of a six-month campaign," that leveraged several attack methods to infiltrate Google's server infrastructure. Google did not reveal the specific services which had been targeted.[139]	
Outcome: The attack was reportedly larger than a similar attack caused by the Mirai Botnet (a form of	

[135] Australia Financial Review, 2021
[136] Ibid
[137] South Australian Government, 2021
[138] ABC, 2021
[139] ZDNet, 2020

malware), which occurred in 2016 and was considered record-breaking at the time. Similarly, this attack was larger than a comparable DDoS attack which targeted Amazon infrastructure in early 2020. While many of the attack's intended effects were successfully mitigated, Google disclosed the occurrence to raise awareness of the increasing number of nation-state hacking incidents, and the high likelihood that DDoS attacks are likely to increase significantly in the coming years.[140]

Identified Gap: Data Centre company Equinix has predicted that, by 2023, there will be a 45% increase in global interconnection bandwidth, creating significantly more opportunity for DDoS and similar cyber-attacks on vulnerable assets.[141] While the potentially detrimental consequences of the DDoS attack on Google were largely avoided, this case study demonstrates the importance of strong risk identification, mitigation, and remediation practices. Rapid increases in interconnectivity and changes to the cyber landscape reinforce the importance of strong, resilient critical cloud assets.

Melbourne's Google Cloud Experiences Outage (2021)	**Physical Risk**

Situation: In August 2021, Google's newest cloud region ('australia-southeast2', located in Melbourne) experienced a 1 hour and 30-minute outage, because of a 'transient voltage' issue, forcing network hardware to be rebooted.[142] Transient voltages are caused by the sudden release of stored energy due to incidents such as lightning strikes, unfiltered electrical equipment, contact bounce, arcing, capacitor bank or generators being switched 'on' and 'off'. The Melbourne Google Cloud had opened in the month prior, intended to help customers in improving business continuity planning and securing IT and business requirements for disaster recovery, while maintaining data sovereignty within Australia.[143]

Outcome: The disruption was reported to have affected any service that uses Cloud Networking, including public IP traffic connectivity, Cloud Storage, Cloud Run, Cloud SQL, and Cloud Filestore, among other services.[144] Google's final analysis of the incident named 23 impact services in total.[145]

Identified Gap: This case study demonstrates the extent to which services can be affected in the event of unforeseen network equipment issues, in this case cause by transient voltage. Google has not confirmed whether the affected equipment belonged to it or a supplier. The case study demonstrates that critical cloud assets of all sizes should seek to understand and mitigate risks in all hazards through their risk management practices.

Data Centre Hack on NordVPN (2018)	**Personnel & Cyber Risk**

Situation: In March 2018, popular private network provider NordVPN was hacked. The attacker gained access to the VPN provider's server by exploiting an insecure remote management system, which NordVPN said it was unaware existed.[146]

Outcome: The breach caused alarm that hackers may have accessed sensitive user data. However, NordVPN stated the compromised server did not contain any user activity logs and that none of its applications send user-created credentials for authentication, so usernames and passwords were protected from interception too. The company also confirmed it had installed intrusion detection systems in response to the attack - a popular technology that companies use to detect early breaches.[147]

Identified Gap: This case study demonstrates that some, even popular, network providers lack the capabilities required to detect and prevent malicious intrusions before they occur.

[140] Ibid
[141] Equinix, 2021
[142] Data Centre Dynamics, 2021
[143] Google Cloud, 2021
[144] Data Centre Dynamics, 2021
[145] Google Cloud, 2021
[146] TechCrunch, 2019
[147] Ibid

Former Employee Attacks Cisco Systems (2018)	Personnel Risk
Situation: In September 2018, a former Cisco employee accessed Cisco Systems' cloud infrastructure, hosted by Amazon Web Services, without Cisco's permission. The former employee admitted that during his unauthorised access he was successful in deleting 456 virtual machines for Cisco's WebEx Teams application, which provides video meetings, video messaging, file sharing, and other collaboration tools.[148]	
Outcome: The former employee's actions caused more than 16,000 WebEx Teams accounts to be shut down for up to two weeks. Cisco was forced to spend approximately $1.4 million (USD) in employee time to restore the damage to the application and refund over $1 million (USD) to affected customers. No customer data was compromised as a result of the attack. The perpetrator was sentenced to 24 months in prison and ordered to pay a $15,000 fine for intentionally accessing a protected computer without authorization and recklessly causing damage.[149]	
Identified Gap: This case study demonstrates the need to screen and maintain awareness of the potential threats posed by current and former employees of critical data assets. This incident highlights the financial impediments and compromised personal data risks which may arise where insufficient employee checks are undertaken or user access is not appropriately controlled.	

[148] United States Department of Justice, 2020

[149] Ibid

Key risks to critical data processing or storage assets

Hazard domain	Identified risk	Example
Physical Natural Hazards	Extreme weather events, resulting in power cuts, power surges, strong winds and flooding, present a substantial threat to critical data assets. Where responsible entities have not undertaken adequate preparation, including waterproofing, ensuring the availability of back-up generators and other business continuity planning, the consequences ensuing from natural disasters can be detrimental. Sensitive data may be lost or compromised.	In 2017, Hurricane Harvey affected large parts of the United States' Texas and Louisiana. In addition to catastrophic flooding and extensive power outages, Telco and ISP Level 3 Communications indicated they had experienced several isolated disruptions to their provision of services. However, Data Foundry provided that its "…purpose-built facility designed to withstand category 5 hurricane wind speeds," meant power had been maintained, and customer access and data preserved.[150]
Cyber	Traditionally, ransomware attacks have not involved theft of personal data – but rather, the encryption of data with access only provided once ransom had been paid. Today, increased sophistication means almost half of all ransomware attacks involve the theft of protected data, before encryption.[151] Critical data assets are particularly vulnerable to the growing threat of ransomware attacks and compromised data.	In 2013, Adobe made an initial report that hackers had stolen nearly 3 million encrypted customer credit card records, along with login details from 38 million 'active users'. The attack had also successfully exposed customer names, debit and credit card information. In August 2015, Adobe was asked to pay $1.1 million in legal fees, and a further $1 million settlement to its customers, after violating US legislation pertaining to customer data, as a result of the infiltration.[152]
Supply Chain	Cloud Service Providers' (CSP) multi-tenancy arrangements, where resources and services are shared between multiple users and customer organisations, can amount to a point of weakness in supply chains. Specifically, multi-tenancy increases the attack surface, leading to an increased chance of data leakage if the separation controls fail. Any vulnerability in a CSP's supply chain can affect the CSP itself, as well as its customers. Compounding this vulnerability is the difficulty associated with assessing supply chain risks – where it is not feasible to vet every vendor, partner and customer. While a CSP may seek to vet relevant policies and procedures, it is difficult to know whether these are fully enforced.	The Cloud Security Alliance has identified a risk associated with the exploitation of software vulnerabilities, which support multi-tenancy. Such exploitation can lead to a failure to maintain separation among tenants.[153] This failure can be used to gain access from one organization's resource to another user's or organization's assets or data. Multi-tenancy increases the attack surface, heightening the change of data leakage where separation controls fail. While no reports of an attack based on separation failures have been reported, proof of concept exploits have been verified.[154]
Personnel	Data centres and CSPs face a two-fold personnel risk: firstly, data breaches may arise where employees accidentally share, misplace or mishandle sensitive data;	Verizon's 2019 Insider Report Threat identified that 57% of database breaches involve insider threats, while 61% of those employees are not in leadership positions when the breach occurred.[156]

[150] Data Centre Dynamics, 2017
[151] Kroll, 2021
[152] CSO, 2021
[153] Sybex, 2016
[154] Carnegie Mellon University, 2018

Hazard domain	Identified risk	Example
	secondly, organisations may be compromised where employees promulgate data theft or data leakages.[155]	Further, in August 2019, personal information of 317 people applying for Australian visas was leaked accidentally. The breach occurred after an email containing the sensitive information was mistakenly sent to a member of the general public, following a typo in the intended recipient's email address.[157] Whilst this was accidental, it does highlight the ease in which a malicious employee could exploit security vulnerabilities.

Existing legislation related to critical data processing or storage assets

Overview of regulation			Identified gaps
Commonwealth	*Criminal Code Act 1995*	Outlines offences and subsequent penalties for computer intrusions, unauthorised modification of data, unauthorised impairment of electronic communications, creation and distribution of malicious software, and dishonesty in obtaining or dealing with financial information.	This Act applies penalties to individuals or groups who may seek to infiltrate critical data assets, rather than the operators of the assets. As such, it does not enable a holistic uplift in the security of critical infrastructure in Australia.
	Public Governance, Performance and Accountability Act 2013	Governs adherence to the Protective Security Policy Framework, which supports the protect Commonwealth entities in securing information.	The Act is limited in its application to Commonwealth entities only. Its exclusion of private, State and Territory entities means it is insufficient to incite a uniform uplift in the security and resilience of critical data assets.
	Privacy Act 1998	This act includes the Australian Privacy Principles and is the principle piece of data protection legislation. It includes mandatory reporting for the unauthorised disclosure of personal data.	While this Act outlined procedural requirements for personal data handling and the reporting of notifiable breaches, it does not require the identification, analysis or mitigation of threats to critical data assets, which would be preventative, rather than reactive, in nature.
	National Archives Act 1983	Establishes and mandates long-term data retention, storage, and access protocols to be followed by Commonwealth agencies.	The Act is limited in its application to Commonwealth entities only. Its exclusion of private, State and Territory entities means it is insufficient to incite a uniform uplift in the security and resilience of critical data assets.

[156] Ibid
[155] Forbes, 2019
[157] Silicon, 2019

Overview of regulation			Identified gaps
New South Wales	*Government Information (Public Access) Act 2009*	Sets out the principles and processes underpinning freedom of information in New South Wales.	The Act does not consider risk management practices for access to and distribution of information and as such, is insufficient to incite an uplift in the security and resilience of critical data assets.
Victoria	*Privacy and Data Protection Act 2014*	Enforces data security frameworks upon the public sector entities, including the requirement to discharge responsibilities under Victoria's Information Privacy Principles The data security framework is intended to protect public data. The Act also mandates compliance with data security standards imposed by the Victorian Information Commissioner.	While the Act and related Principles includes a risk assessment component, including the undertaking of a security risk profile assessment, it is limited in its application. Its exclusion of private entities means it is insufficient to incite a uniform uplift in the security and resilience of critical data assets.
Queensland	*Information Privacy Act 2009*	Mandates Government agencies' adherence to Queensland's Information Privacy Principles and Australia's National Privacy Principles.	The Act is limited in its application to Government agencies only. Its exclusion of private entities means it is insufficient to incite a uniform uplift in the security and resilience of critical data assets.
Western Australia	*Freedom of Information Act 1992*	Sets the requirements for parties wishing to view or amend documents containing personal information in Western Australia.	The Act is limited in its application to Government agencies only. Its exclusion of private entities means it is insufficient to incite a uniform uplift in the security and resilience of critical data assets.
Northern Territory	*Information Act 2002*	Sets out the principles and processes underpinning freedom of information in the Northern Territory.	The Act does not consider risk management practices for access to and distribution of information and as such, is insufficient to incite an uplift in the security and resilience of critical data assets.
Tasmania	*Personal Information and Protection Act 2004*	Sets out the principles and processes underpinning freedom of information in Tasmania.	The Act does not consider risk management practices for access to and distribution of information and as such, is insufficient to incite an uplift in the security and resilience of critical data assets.

Existing standards, guidelines and regulators for critical data processing and storage assets

Hazard domain	Organisation	Standards & guidelines
Cyber	Australian Cyber Security Centre	**Information Security Registered Assessor Program (IRAP):** for government data
		Cyber Security Guidelines
		Cloud computing Security for Cloud Computing Providers
	Office of the Victorian Information Commissioner	**Information Privacy Principles (Vic)**

	European Union	**GDPR**
		NIS Directive
	Secretary General of the Council of Europe	**Budapest Convention on Cybercrime**
	Attorney-General's Department Australia	**Protective Security Policy Framework**
Physical	Attorney-General's Department Australia	**Protective Security Policy Framework**
Personnel	Attorney-General's Department Australia	**Protective Security Policy Framework**
	Standards Australia	**AS 4811-2006**
	Australian Cyber Security Centre	**Information Security Manual**
Supply Chain	APRA	**CPS 231, 234**
	Australian Cyber Security Centre	**Supply chain Guidance for Practitioners**

Jurisdiction	Regulator/s
Commonwealth	*Office of the Australian Information Commissioner*
Australian Capital Territory	*Office of the Australian Information Commissioner*
New South Wales	*Information and Privacy Commission New South Wales*
Northern Territory	*Office of the Information Commissioner Northern Territory*
Queensland	*Queensland Office of the Information Commissioner*
South Australia	*South Australian privacy committee*
Tasmania	*Tasmanian Ombudsman*
Victoria	*Office of the Victorian Information Commissioner*
Western Australia	*Office of the Information Commissioner (WA)*

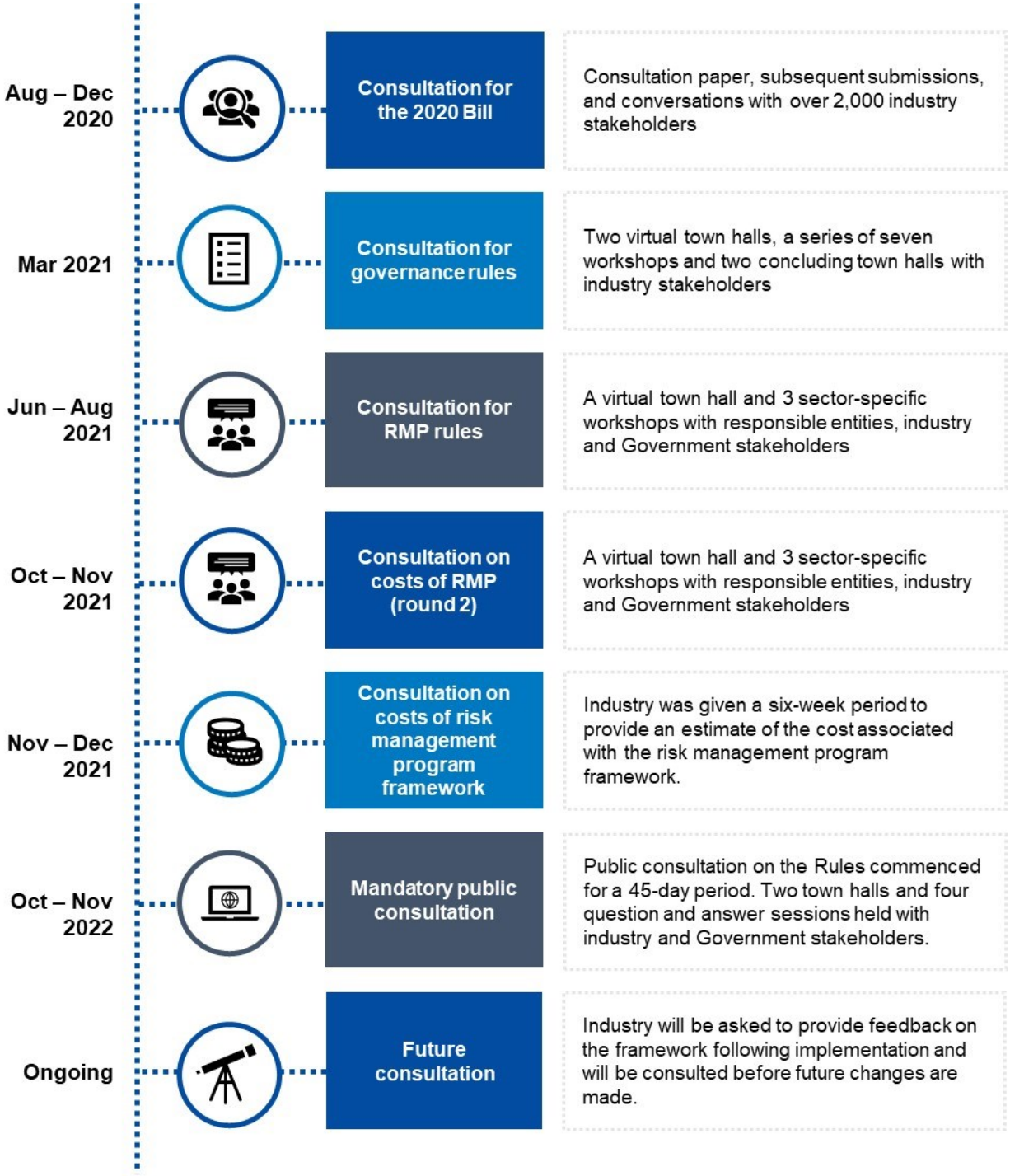
Additional information on consultation

Overview of stakeholders consulted

Stakeholders Consulted	
• AirTrunk Operating Pty Ltd	• Macquarie Telecom Group Ltd
• AUCloud	• Microsoft Pty Ltd
• Australian Data Centres	• NEXTDC Ltd
• Amazon Web Services Australia Pty Ltd	• Office of the Australian Information Commissioner
• CDC Data Centres	• Singtel Optus Pty Ltd
• Cenitex	• Palo Alto Networks, Inc.
• Cisco Systems Inc.	• Pulse DC
• CommandHub Pty Ltd	• SAP SE / SAP Australia Pty Ltd
• Communications Alliance Ltd	• TasNetworks Pty Ltd

- Equinix, Inc.
- Geoscape Australia
- Google Australia Pty Ltd
- IBM Australia, Ltd
- Infosys Ltd
- Macquarie Group Ltd
- Teradata Corporation
- Protiviti Inc.
- Leidos Australia
- Oracle Corporation
- Integrated Marine Observing System (IMOS)
- Australian Information Industry Association (AIIA)
- SoftIron Australia Pty Ltd
- 21e8
- Global Switch Australia Pty Ltd
- Verizon Australia Pty Ltd
- Telstra Corporation Ltd
- The Gateway Networks Governance Body
- Vault Cloud
- VMWare, Inc.
- Vocus Group Limited
- Splunk Inc.
- Forcepoint
- Cybersult Pty Ltd
- Saleforce
- Cygence Llc
- Datapod (Australia) Pty Ltd
- Atlassian Corporation Plc
- APNIC Pty Ltd
- ServiceNow, Inc.
- HERE Technologies
- Dell Technologies Inc.
- DCI Data Centers
- Healy Advisory Pty Ltd

Consultation timeline



RMP Rules consultation

Consultation with industry stakeholders occurred across the following key stages:

1. **A virtual town hall**, held in June 2021 attended by approximately 150 industry and Government stakeholders, to communicate the purpose of the consultation process and obtain information to inform the design of future workshops.
2. **A series of three virtual workshops**, held over a five-week period beginning in July 2021 and each attended by approximately 140 industry and Government stakeholders, which provided a forum to consult on RMP rules and assisted in understanding the costs and benefits associated with implementing the RMP framework. Workshops were designed to provide:
   i. Several opportunities for discussion and feedback to gather industry perspectives;
   ii. Polling, in-session surveys and facilitated discussions; and
   iii. 'Break out room' discussions to ensure comprehensive discussion occurred across all subsets of industry.
3. **Out of session consultation**, including meetings with a number of stakeholders and extensive email communication.
   – Stakeholders were encouraged to contact the Department out of session. The Department availed itself to stakeholders to discuss their concerns, working to ensure stakeholders' understanding of the rules, and the rules' proportionality.
   – Out of session engagement also assisted in the iterative development of rules between workshops, through addressing concerns raised by individual stakeholders and proposing a solution.
   – This engagement strengthened the relationship between the Department and industry, while providing insights on implementation costs, entities' operating environments and the overall impacts of the proposed regulatory changes.
4. **Three follow-up Consultation Sessions and two Industry-agnostic Town Hall** held in October and November 2021. The purpose of the consultation sessions was to provide an update for industry on the move from sector-specific to sector-agnostic RMP rules, to gain sector-specific feedback on the updated RMP rules, and to gain feedback on the new asset definition for critical data storage and processing assets. The purpose of the Industry Town Hall was to present the updated RMP rules and provide information on the further consultation period. The two consultation sessions were attended by approximately 75 and 60 industry and Government stakeholders respectively. The Town Hall was attended by approximately 800 industry and Government stakeholders across the 10 critical infrastructure sectors, including by many stakeholders from the data storage and processing sector.
5. **Mandatory Public Consultation**, following the Minister commencing a 45-day consultation period on 5 October 2022 (the mandatory period is 28 days). Consultation included two Town Hall Sessions held on 10 October and 12 October 2022, attended by approximately 550 industry and Government stakeholders (across both sessions). The sessions provided information on the proposed RMP Rules as well as the broader obligation. These Town Halls, as well as four subsequent question and answer sessions, provided an opportunity for industry to ask questions about the proposed RMP Rules and process.

The consultation roadmap on the RMP rules, pictured in the figure below, provides additional insights on the topics for discussion at each consultation phase.

Key themes from consultation

Rule category	Identified themes		Impact on development of rules
Sector-agnostic RMP Rules	**Consultation Sessions**	• Industry believes the RMP Rules are **clear and understandable.** • Industry believes the RMP Rules will **be able to be implemented.** • The RMP Rules provide a **baseline** for sector resilience and security. • There is an **appetite for guidance material** to support sector-specific uplift in security and resilience. • Industry believe the RMP Rules will **better facilitate alignment** between interdependent critical infrastructure sectors.	In response to feedback received during the consultation sessions, the Department committed to: • The development of guidance materials, which would highlight aspects of risk management that should be prioritised by responsible entities and assist industry in interpreting and implementing the rules to achieve an uplift in security and resilience.

Consultation on costs

During the second information session, attendees were invited to participate in cost impact data collection through the completion of a cost impact template. This template was designed to collect substantive costing data to supplement the anecdotal costing discussions which had occurred throughout the workshop series. Industry were asked to provide:

- Their demographic information;
- Effort and cost estimates split by one-off and ongoing costs, staff effort, capital and other operating costs, and an estimated range between expected costs and highest possible costs; and
- Any comments on key boundaries, assumptions and cost drivers attached to the costing estimates provided.

Industry was provided with the template on 29 November 2021, with submissions open for a period of 4 weeks and closing on 24 December 2021.

The absence of entities within the sector that meet the definition of a small business indicated that consultation with the Australian Small Business and Family Enterprise Ombudsman was not required to identify expected costs to small businesses in preparing this RIS.[158]

[158] Office of Best Regulation Practice (2021).

Appendix K: Supplementary information for critical broadcasting assets

Overview of the role of broadcasting in Australia

The broadcasting asset class of the communications sector is comprised of radio and television (free-to-air) broadcasters and plays a particularly important role in emergency management through the provision of forecasts and regular updates. Radio involves companies broadcasting audio signals using radio (electromagnetic) waves of frequencies between 30 hertz (Hz) and 300 gigahertz (GHz) to transmit programming. These are generated by an electronic device called a transmitter which is connected to an antenna, which radiates the waves, and is received by a radio receiver which is connected to another antenna[159]. The key providers of radio communications include Southern Cross Austereo (26% market share), Australian Broadcasting Corporation (ABC) (21% market share) and Here, There, Everywhere (14% market share).

Television broadcasting refers to companies broadcasting visual content using over-the-air transmission networks. Unlike cable or satellite television, viewers of broadcast television do not have to pay to receive the programming. As a result, there are few non-advertising revenue sources for television broadcasters. This situation suits local stations, because they are doing quite well with four sources of advertising money: their share of national network advertising, their sale of advertising time during their own programming (mostly local news), their sale of advertising time during programming that they purchase from non-network sources (e.g., reruns of Seinfeld or new episodes of Oprah Winfrey), and their sale of local commercials during some pauses in network programming. Major providers include Seven West Media (28% market share), Nine Entertainment (25% market share) and Network Ten (14% market share).

Broadcast media play an important role in emergencies and national campaigns, both in disseminating and collecting information. As Australia's economy expands, the need for heightened security and resilience in Australia's critical broadcasting assets is increasing.

The SOCI Act refers to assets within a critical infrastructure sector as 'critical infrastructure assets'. Section 12E of the SOCI Act proves the following in relation to 'critical broadcasting assets':

*12E Meaning of **critical broadcasting asset**:*

1) *One or more broadcasting transmission assets are a **critical broadcasting asset** if:*
   a) *the broadcasting transmission assets are:*
      i. *owned or operated by the same entity; and*
      ii. *located on a site that, in accordance with subsection (2), is a critical transmission site; or*
   b) *the broadcasting transmission assets are:*
      i. *owned or operated by the same entity; and*
      ii. *located on at least 50 different sites; and*
      iii. *not broadcasting re-transmission assets; or*

[159] NASA, "What are radiowaves," (2018), accessed at < https://www.nasa.gov/directorates/heo/scan/communications/outreach/funfacts/txt_radio_spectrum.html>

c) the broadcasting transmission assets are owned or operated by an entity that, in accordance with subsection (3), is critical to the transmission of a broadcasting service.

Note: The rules may prescribe that a specified critical broadcasting asset is not a critical infrastructure asset (see section 9).

2) For the purposes of paragraph (1)(a), the rules may prescribe:

a) specified sites that are critical transmission sites; or

b) requirements for sites to be critical transmission sites.

3) For the purposes of paragraph (1)(c), the rules may prescribe:

a) specified entities that are critical to the transmission of a broadcasting service; or

b) requirements for an entity to be critical to the transmission of a broadcasting service.

The Department, on 23 May 2021, published a policy paper Protecting Critical Infrastructure and Systems of National Significance – Draft Critical Infrastructure Asset Definition Rules (2021) (the Policy Paper). In the Policy Paper,[160] the Department states its intention to recommend the Minister make rules prescribe assets that are owned or operated by TX Australia to be critical broadcasting assets, as TX Australia services a variety of major broadcasters, which otherwise do not meet the 'at least 50 sites' threshold under section 12E(b)(ii) of the Act.

TX Australia is a major broadcast transmission operator and provides television transmission for broadcasters, including for commercial metropolitan television networks Seven, Nine and Ten. TX Australia will not be expected to be captured by the 'at least 50 sites' threshold. It is expected that BAI Communications will be captured by the 'at least 50 sites' threshold'. BAI Communication is appointed to operate and maintain the broadcast network for the ABC, the Special Broadcasting Service (SBS), Network 10, Southern Cross Australian Austereo and the NSW Public Safety Network.

Impacts of a disruption to critical broadcasting assets

The consequences of a prolonged and widespread disruption to a critical broadcasting asset may include:

- Disruption to telecommunication networks and live broadcasting services
- Disruption in emergency telecommunication arrangements and information for community preparedness and responsibility in times of emergency
- Inability for businesses and governments to function as normal
- Disruption to network coverage and consumers services
- Breach of privacy and customer data
- Unauthorised access to communication channels for surveillance and incorporating malicious software
- Disruption to IT services, systems and business operations
- Disruption to information sharing to public on current, domestic and international affairs.

[160] Home Affairs, 2020

Examples of disruptions to critical broadcasting assets – domestic and international

In the summer of 2020, the ABC's radio and TV networks sustained heavy damage from the bushfire crisis across NSW and Victoria, forcing the national broadcaster to call on the military and members of the public to maintain emergency broadcasting. The transmitter in the South Coast of NSW, melted and communications and the community were unable to receive or transmit radio coverage.[161] The transmitter equipment took months to repair before it became completely operational again. This resulted in the community not receiving proper coverage and relying on interim measures, and even then, services were not at full capacity. The cost of restoring the infrastructure was between $1.5 million and $2 million.[162] This demonstrates that broadcast towers remain as the 'weakest' link during emergency broadcasts as the infrastructure is vulnerable to fires. Communicating accurate emergency information is vital and can disrupt other sectors when there is not transmission of information available.

Other past incidents, in both Australia and overseas, demonstrate the potentially severe, cascading consequences of prolonged disruption in any critical infrastructure sector – for that sector itself, for other critical infrastructure sectors, and for the affected national economy. The following series of case studies, each categorised by its relevant hazard domain or domains, demonstrate these consequences, in the context of critical broadcasting assets. While some are drawn from overseas, these case studies highlight a clear imperative for decisive action, in order to prevent the occurrence of similar, or further, incidents for Australia's critical broadcasting assets.

Channel Nine Network Cyber Attack	**Cyber security**
Situation: On 29 March 2021, the Nine Network became the target of Australia's largest cyber-attack on a media company. For more than 24 hours, the cyberattack affected digital production systems and impaired Channel Nine's ability to broadcast from its Sydney studios, forcing the network to relocate operations to its Melbourne studios.	
Outcome: As a result of the attack, data and production systems were temporarily unavailable. Additionally, the cyber-attack impacted regular news bulletins and impeded the Australian Financial Review, The Sydney Morning Herald, and The Age's ability to publish. According to estimates, the cyber-attack on the network is expected to cost the network more than $1 million dollars, in addition to significant recovery expenses.	
Identified Gap: The Nine Network engaged with the Australian Signals Directorate (ASD) to determine the source of the attack, which remains unsolved. It was indicated that several computers displayed unusual behaviour by 'working harder' than would be expected prior to the attack. The network spoke with forensics and recovery experts and determined that the attacker utilised Nine systems to distribute fraudulent updates to employees' devices. These upgrades encrypt data and make devices unresponsive. Without sufficient protections and continuous re-evaluation, operating systems considered critical to defending against catastrophic events, may be compromised.	

[161] McCutcheon, 2020

[162] Ibid

France TV5Monde Cyber Attack	Cyber security, personnel
Situation: In April 2015, TV5Monde, one of France's largest television networks with an international reach in more than 200 countries, experienced the largest cyberattack ever against a television network. Highly targeted malware was used to destroy the TV network's systems, and all 12 of its channels were taken off the air.[163] The network was accessed on 23 January 2015, and the attackers remained hidden for months while conducting reconnaissance of the network, which is a common method for cyber-attacks looking for weaknesses in the network and associated systems.	
Outcome: The Network had a three-hour outage during which it was unable to generate news programming. Additionally, the hackers posted documents and messages on TV5Monde's Facebook page pretending to be the families of French soldiers participating in anti-Islamic State Group operations, as well as posting threats against the troops. The cost of the attack was 5 million Euro in 2015 (8 million AUD) and 11 million Euro (18 million AUD) over the next three years – a total of more than 16 million Euro (26 million AUD).[164]	
Identified Gap: According to the investigation, the hackers used a social engineering technique; after journalists interacted with a phishing email, the hackers were able to breach the channel's network via a Trojan horse, spread the virus throughout the IT infrastructure, and create accounts with administrator privileges. The V5 Monde multimedia servers were open to the internet through their remote desktop protocol port and were utilising the default username/password combination.	

ABC's south coast transmitter – Australia's summer bushfires	Physical and natural hazard
Situation: The Australian bushfires that devastated the South Coast of New South Wales (NSW) in the summer of 2020 caused widespread devastation and panic, as the transmitter in the region melted. Communications with residents in the community were impaired by the inability to receive or transmit radio coverage.[165]	
Outcome: The transmitter equipment took months to repair before it was completely operational again. The cost of restoring the infrastructure owned by BAI Communications Australia, which provides the broadcast towers to ABC on a commercial arrangement, was between $1.5 million and $2 million.[166]	
Identified Gap: The ABC's managing director stated that the burn out damage demonstrates the critical necessity for AM radio technology and that a backup generator should be maintained and in full operation to assist in getting information out during disasters like these. The analysts have been adamant that it is crucial that future infrastructure is as resilient as possible as broadcast towers still remain the weakest link during emergency broadcasts.	

Sinclair Broadcast Group TV Network Cyber Attack	Cyber security
Situation: Sinclair Broadcast Group (SBG), one of the leading television operators in the United States of America, was the target of a ransomware attack that disrupted television stations across the country, including office and operational networks. According to initial reports, the attack was planned by the cybercrime group Evil Corp.[167] The hackers attacked the broadcasting organisation with malicious code.	

[163] Corera, 2016
[164] Ibid
[165] Lauder, Reardon, McCutcheon, 2020
[166] Ibid
[167] Butts, 2021

Outcome: The cyber-attack disrupted the workflow of the broadcasting group's several stations, including certain areas of its distribution of local advertising. Employees were unable to access emails, phones, video files, or graphics. Additionally, SBG acknowledged that data was stolen from the company's network.

Identified Gap: It has been reported that the ransomware attack was preceded by a call for a password reset across all of Sinclair which highlighted a serious network issue. Sinclair's CEO has stated that it will look for immediate opportunities to enhance the current existing security measures. This attack demonstrates that the IT infrastructure remains a high target for hackers, and that protection on all surfaces of television networks is necessary to stop hackers stealing data and information.[168]

Key risks to critical broadcasting assets

Hazard domain	Identified risk	Example
Physical	In times of crisis, Australians rely on broadcasting services to keep people informed of significant national events and crucial information during times of disaster. However, catastrophic weather occurrences such as the late 2019 and early 2020 bushfires demonstrate physical broadcasting transmitters are now under more threat and in risk of disruption, particularly in regional locations.	Around August 2021, the Bilsdale transmitting station (broadcasting and telecommunications facility) based in Helmsley, North Yorkshire, England, a fire started at the complex and it was reported up to one million homes had lost TV and radio signals.[169] A temporary mast has been put in place until full repairs are made by 2022, meaning the majority of people have some form of working signal but not full coverage.
Cyber	Broadcasting services are increasingly relying on IP networks and IT for content production, storage and delivery, which inevitably leads to a much wider exposure of vulnerabilities. This makes such attacks extremely difficult to prevent, identify or mitigate in real time, which is essential in the broadcasting sector where latency can be a major issue.[170]	In April 2015, a cyber attack occurred on the French International TV broadcaster, TV5Monde. The network, which is available in 200 countries, came under attack from a group claiming to be the 'Cyber Caliphate'. The attack took the broadcaster's 12 channels off the air and according to its director-general, nearly led to the destruction to all of its systems.
Supply Chain	The physical supply chain and digital supply chain have presented difficulties, in particular during the COVID-19 pandemic. In particular, the broadcasting organisations are confronted with additional major interruption. They must navigate both supply- and demand-side restrictions, which have an effect on the economics that support their capacity to commercialise content.	The COVID-19 pandemic has incited concern of disruption of digital supply chain required for the broadcast infrastructure to continue services and transmission coverage.
Personnel	When personnel are unable to operate due to events beyond their control, critical broadcasting systems and operations may suffer significant delays or shuts down. Additionally, employees having access to	A former journalist at the ABC, published stories based on leaked Government documents. The stories were based on hundreds of pages of Secret Defence documents provided by an insider and considered as a threat to national

[168] Ibid

[169] Williams, Robinson, 2021

[170] Fachot, 2019

Hazard domain	Identified risk	Example
	systems, data, or premises may offer insider threat concerns such as fraud, theft, intelligence, infrastructure sabotage, and data misuse.	security given the stolen information that was published.[171]

Existing legislation related to critical broadcasting assets

Overview of regulation		Identified gaps
Broadcasting Services Act 1992 (Cth)	The Act outlines the legal framework of Australian broadcasting, including community broadcasting, and explains the role the sector plays in delivering diverse media services that reflect a sense of Australian identity, character and cultural diversity. The law stipulates what is political advertising and the specific conditions which must be met before they are authorised for publication.	While the Act carries out various fundamental principles such as the security standards, best practices and governance, it does not, however, have a risk management approach towards cyber-attacks, resilience risk and protection on broadcasting services and the broadcasting infrastructure.
Telecommunications (Interception and Access) Act 1979 (Cth)	The Act makes it an offence for a person to intercept or access private telecommunications without the knowledge of those involved in that communication. The TIA Act permits access to communications content for law enforcement and national security purposes.	While the Act is effective considering technological developments and changes in the structure of communication industries, it lacks a risk management approach to prevent cyber security and other incidents to protect data.
The Community Broadcasting Codes of Practice (The Codes)	The Codes set out the guiding principles and policies for programming on community broadcasting stations. They also outline the operational standards for stations that hold a community broadcasting licence. The Codes do not replace the licence conditions in the Act; they are complementary, and stations are legally obliged to follow both the licence conditions and the Codes.	While the Codes protect the licences and provide policies for programming of broadcast stations, it lacks a solid risk management strategy to prevent security and resilience risk that might compromise national broadcasting. Additionally, it lacks a clear approach for protecting the broadcasting stations' data.
Radiocommunications Act 1992 (Cth)	The Act aims to promote the long-term public interest derived from the use of spectrum. It does so by providing for the management of spectrum in a manner that: • Facilitates the efficient planning, allocation and use of spectrum. • Facilitates the use of spectrum for commercial and defence purposes, national security purposes and other noncommercial purposes. This includes public safety and community purposes. Supports the communications policy objectives of the Australian Government.	While the Act establishes a framework for defence and national security purposes, it does not address foreign intervention, structural damage, or a cyber security and other incidents approach to the broadcasting infrastructure. This puts the transmitter infrastructure and signals at risk of major disruptions.

[171] Cockburn, 2019

Overview of regulation		Identified gaps
Australian Communications and Media Authority (ACMA)	ACMA is responsible for regulating telecommunications and radio communications, including promoting industry self-regulation and managing the radiofrequency spectrum. The ACMA also has significant consumer protection responsibilities.	While the ACMA establishes regulations and standards for broadcast networks, manages licences, and monitors compliance, it lacks a systematic approach to defending networks and infrastructure from cyber security and other incidents threats.
Australian Competition & Consumer Commission (ACCC)	An independent Commonwealth statutory authority whose role is to enforce the *Competition and Consumer Act 2010* and a range of additional legislation, promoting competition, fair trading and regulating national infrastructure for the benefit of all Australians.	The ACCC provides a framework for regulating national infrastructure, however there isn't a risk management approach to cyber security incidents and reporting to avoid disruptions to broadcasting services and supply chain.

Existing standards, guidelines and regulators for critical broadcasting assets

Hazard domain	Organisation	Standards & guidelines
Cyber	International Organization for Standardization (ISO)	**ISO 27001** provides requirements for information security management systems.
	National Institutes of Standards and Technology (NIST)	Cybersecurity Programs
Physical	Standards and codes for TV and radio broadcasters	**Broadcasting Services (Australian Content in Advertising) Standard 2018** **Broadcasting Services (Commercial Radio Current Affairs Disclosure** **ACMA documentary guidelines 2021**

Jurisdiction	Regulator/s
Commonwealth	Australian Communications and Media Authority (ACMA) Australian Competition and Consumer Commission (ACCC)
Australian Capital Territory	ACMA
New South Wales	ACMA
Northern Territory	ACMA
Queensland	ACMA
South Australia	ACMA
Tasmania	ACMA
Victoria	Consumer Affairs Victoria
Western Australia	ACMA

Additional information on consultation

Overview of stakeholders consulted

Stakeholders Consulted
• BAI Communications Australia • TX Australia

RMP Rules consultation

The Department undertook extensive consultation with industry, including the broadcasting sector for the design of RMP rules, with the objectives of:

- Assessing whether there are existing regulations that meet the Bill's risk management program objectives, to ensure the regulatory burden is reduced where possible; and
- Ensuring there are rules in place that will drive an uplift in the security and resilience of critical broadcasting assets.[172]

Consultation with industry stakeholders occurred across the following key stages:

1. **A virtual Town Hall**, held on 19 October 2021, attended by 360 approximately industry and Government stakeholders, including from the broadcasting sector. The purposes of the session were to:
    i. Outline the CI/SONS reforms and provide an update on the SLACI Bill (now SLACI Act) and SLACIP Bill (now SLACIP Act);
    ii. Provide an update for industry on the decision to consult on sector-agnostic RMP rules (as opposed to sector-specific rules), and outline how this would affect the consultation process going forward; and
    iii. Answer any questions about the Bills or RMP rules consultation process.
2. **Two broadcasting-specific Information Sessions,** held on 28 October and 16 November 2021, attended by approximately six industry and Government stakeholders. The purpose of the information sessions was to reiterate the update for industry on the move from sector-specific to sector-agnostic RMP rules and to gain sector-specific feedback on the RMP rules.
3. **A wrap-up virtual Town Hall** held on 25 November 2021. The purpose of the Town Hall was to present the updated RMP rules and provide information on the further consultation period. The Town Hall was attended by approximately 800 industry and Government stakeholders across the 10 critical infrastructure sectors, including by stakeholders from the broadcasting sector.
4. **Out of session consultation:**
    – Stakeholders were encouraged to contact the Department out of session. The Department availed itself to stakeholders to discuss their concerns, working to ensure stakeholders' understanding of the rules, and the rules' proportionality.
    – Out of session engagement also assisted in the iterative development of rules between workshops, through addressing concerns raised by individual stakeholders and proposing a solution.

[172] Department of Home Affairs 2021, 2

– This engagement strengthened the relationship between the Department and industry, while providing insights on implementation costs, entities' operating environments and the overall impacts of the proposed regulatory changes.

5. **Mandatory Public Consultation**, following the Minister commencing a 45-day consultation period on 5 October 2022 (the mandatory period is 28 days). Consultation included two Town Hall Sessions held on 10 October and 12 October 2022, attended by approximately 550 industry and Government stakeholders (across both sessions). The sessions provided information on the proposed RMP Rules as well as the broader obligation. These Town Halls, as well as four subsequent question and answer sessions, provided an opportunity for industry to ask questions about the proposed RMP Rules and process.

Key themes from consultation

Rule category	Identified themes		Impact on development of rules
RMP rules	**Information sessions**	• The broadcasting sector **broadly agrees** with the RMP rules as drafted. • The broadcasting sector has various levels of risk maturity at current. • There is an **appetite for guidance material** to support sector-specific uplift in security and resilience, especially with regards to meeting the supply chain rules.	In response to feedback received during the information sessions, the Department committed to: • The development of guidance materials, which would highlight aspects of risk management that should be prioritised by responsible entities and assist industry in interpreting and implementing the rules to achieve an uplift in security and resilience.

Consultation on costs

During the second information session, attendees were invited to participate in cost impact data collection through the completion of a cost impact template. This template was designed to collect substantive costing data to supplement the anecdotal costing discussions which had occurred throughout the workshop series. Industry were asked to provide:

- Their demographic information;
- Effort and cost estimates split by one-off and ongoing costs, staff effort, capital and other operating costs, and an estimated range between expected costs and highest possible costs; and
- Any comments on key boundaries, assumptions and cost drivers attached to the costing estimates provided.

Industry was provided with the template on 17 November 2021, with submissions open for a period of four weeks and closing on 15 December 2021.

The absence of entities within the sector that meet the definition of a small business indicated that consultation with the Australian Small Business and Family Enterprise Ombudsman was not required to identify expected costs to small businesses in preparing this RIS.[173]

[173] Office of Best Regulation Practice, 2021

Appendix L: Supplementary information for critical financial market infrastructure assets (payment systems)

Overview of the role of payment systems in Australia

Financial market infrastructures are key components of the financial system. They deliver services critical to the smooth functioning of financial markets and financial stability.[174] Australian financial market infrastructures support transactions in securities with a total annual value of $18 trillion and derivatives with a total annual value of $185 trillion (figures reflect the value of securities trades and notional value of derivatives trades for the year to 31 December 2019). A significant disruption to financial market infrastructures would have a detrimental impact in terms of public trust, financial stability and market integrity and efficiency. The reasons for this include their central position within the financial system and inability of participating financial institutions and, in most cases, consumers and businesses to leverage substitute services.[175]

Payment systems are arrangements through which individuals, businesses and government entities transfer funds between each other. The smooth functioning of payment systems is important for economic activity and financial stability, and payment information is subject to both integrity and confidentiality risks.

There are six clearing streams for payment systems in in Australia:

- Paper (cheques);
- Bulk electronic (direct entry and BPAY);
- Consumer electronic (ATM, cards and point of sale);
- High value electronic (RTGS);
- Cash (notes and coins); and
- The New Payments Platform (delivering single credit transfers).

Specified consumer electronic clearing systems and the New Payment Platform are considered to be critical infrastructure for the purposes of the SLACI Act and SLACIP Act. Disruptions to these retail payment systems would have significant flow-on effects to other parts of the Australian economy.

The lifecycle for transactions through these payments systems involves the following activities:

- **Authorisation** data is transferred between the merchant and issuer financial institutions through the payment system's secure gateways.
- The payment system's designated **clearing** bank then clears the payment with the issuer financial institution through checking that the necessary funds are available.
- **Settlement** data is then transferred between the issuer and merchant financial institutions through the secure gateway to allow for the payment to be credited to the merchant's account.

These payment systems rely on telecommunication networks to provide the rails to process transactions.

The SOCI Act refers to assets within a critical infrastructure sector as 'critical infrastructure assets'. Section 12D of the SOCI Act provides the following in relation to 'critical payment systems':

[174] RBA n.d.

[175] Critical Infrastructure Centre, 2020, p. 21

(4) *An asset is a **critical financial market infrastructure asset*** if it is:

…

(i) An asset that is used in connection with the operation of a payment system that, in accordance with subsection (6), is critical to the security and reliability of the financial services and markets sector.

Note: the rules may prescribe that a specified critical financial market infrastructure asset is not a critical infrastructure asset (see section 9).

…

(6) For the purposes of paragraph (1)(i), the rules may prescribe:

(a) specified payment systems that are critical to the security and reliability of the financial services and markets sector; or

(b) requirements for a payment system to be critical to the security and reliability of the financial services and markets sector

*(7) For the purposes of this section, **Australian body corporate** means a body corporate that is incorporated in Australia.*

The Department, on 23 May 2021, published a policy paper Protecting Critical Infrastructure and Systems of National Significance – Draft Critical Infrastructure Asset Definition Rules (2021) (the Policy Paper). In the Policy Paper, the Department states that it intends to recommend that the Minister make rules to prescribe specified payment systems that are critical to the security and reliability of the financial services and markets sector, including:

a. The Mastercard debit and credit card systems,

b. The Visa debit and credit card systems,

c. The EFTPOS card system, and

d. The New Payments Platform.

Impacts of a disruption to payment systems

The consequences of a prolonged and widespread disruption to a critical payment system may include:

- Disruption to transactions, causing reduced economic activity due to disruption of banking, finance and retail sectors (for example, retail customers may be unable to complete routine transactions such as purchasing groceries or paying utilities bills);
- Disruption to the reliability of the supply of food and groceries, as transactions along the supply chain are disrupted;
- Disruption to transport infrastructure, as ticket sales are disrupted; and
- Reduced public confidence in payment services and key providers, and potentially the broader financial system.

Examples of disruptions to payment systems assets – domestic and international

Westpac, ANZ and Coles-Myer Suffer Boxing Day Technical Difficulties (2018)	Physical & Supply Chain Risk

Situation: On Boxing Day of 2018, Westpac and ANZ EFTPOS machines and mobile banking applications experienced significant malfunctions throughout the day, while Coles-Myer Group gift cards were unable to be accepted. Consumers intending to use Coles-Myer Gift Cards were informed that the organisation's third-party gift card provider was experiencing technical difficulties, resulting in the decline of all Coles-Myer gift cards.

Outcome: ANZ was able to restore its services by Boxing Day evening. However, Westpac's EFTPOS issues were unable to be rectified before the end of the day.[176] A spokesperson for Myer provided that their gift card issue was resolved by 5:30pm on Boxing Day evening.[177] The outages came on a day when Australians were expected to spend as much as $2.62 billion as a result of Boxing Day sales.[178]

Identified Gap: In addition to the inconvenience experienced by customers hoping to take advantage of Boxing Day sale campaigns, this case study demonstrates the importance of payment system organisations having in place sufficient contingency arrangements in the event of an outage. Further, in the case of Coles-Myer, it is important that organisations secure their supply chains so as to limit the impacts of any interruptions experienced by third party providers.

NAB Experiences Nationwide Service Disruption (2018)	Physical Risk

Situation: In early 2018, NAB experienced extended outages across its internet and mobile banking, ATMs and eftpos, with disruptions lasting almost seven hours on a Saturday. The NAB disruption also affected customers across the Tasman, with NAB subsidiary Bank of New Zealand tweeting that its systems were down for part of Saturday morning.[179]

Outcome: An NAB Business executive general manager Cindy Batchelor said the outage was caused by a power issue in the bank's mainframe in Melbourne. The bank said it would compensate customers '100 per cent' for any losses incurred, with people cashless and small businesses unable to process transactions on a busy trading day.[180] NAB's compensation payments cost a total of $7.4 million.[181] Following the incident, NAB said it strengthened 'many of its operational processes; to prevent a similar situation in the future.[182]

Identified Gap: This case study demonstrates the need for consistent awareness and where necessary, upgrades to system capabilities and security, in order to mitigate disruptions to digital payment capabilities. While gaps in the resilience of critical payment assets can cause extended disruptions to affected customers, such events can also result in large financial impediments for the critical assets themselves.

Major Banks Experience Denial of Service Attack (2021)	Cyber Risk

Situation: Australia's major banks' internet services and payment terminals, as well as those of other major

[176] Colangelo, 2018
[177] Colangelo, 2018
[178] Chapman, 2019
[179] Motherwell, 2018
[180] Motherwell, 2018
[181] Smith, 2018
[182] Smith, 2018

Australian brands, experienced outages on 17 June 2021. The outage was due to an issue with technology company Akamai's distributed denial of service (DDoS) mitigation platform 'Prolexic'.[183] The Commonwealth Bank of Australia, Westpac and ANZ, as well as Virgin Australia and the Australian Postal Service, experienced website and online service failures.

Outcome: While the enduring impacts of this attack were minimal, essential payment, travel and postal service did experience intermittent disruption, causing inconvenience to customers and questions as to the security of such services' critical assets. In more extreme cases, DDOS attacks can disrupt services for prolonged periods, impede proper website or application functions and even take an entire business offline.[184]

Identified Gap: This case study highlights the importance of risk mitigation and preparation efforts in securing a payment systems organisation's services. Ensuring secure network set-ups, sufficient distribution and diversification of critical assets and adequate network redundancies are imperative for reducing the effects of a DDoS attack on critical payment system organisations.

Key risks to payment systems assets

Risk	Identified Risk	Example
Cyber	Payment systems are highly reliant on software and information systems. As a result, cyberattacks on these systems can prevent or delay a wide range of economic activity from occurring, causing significant economic disruption. These attacks are growing in frequency and sophistication. Broadly, there are four types of attacks:[185] • Data breaches, where the attacker aims to steal sensitive information; • System disruptions, where attackers disrupt availability of critical systems/websites (e.g., DDoS attacks); • Integrity of data attacks, where attackers try to modify data and render it useless; and Financial attacks, where attackers use fraud or ransom to try to achieve financial gain.	In September 2021, ANZ's online banking services and app suffered outages as a result of a DDoS attack. The outages affected the availability of these services for three days, causing significant disruption to consumer activity.[186]
Supply Chain	Payment Systems may rely on third party services. For example, telecommunications networks often provide the rails to process transactions between secure gateways. Where a critical third-party service becomes unavailable or is compromised, payment systems may be disrupted.	As referenced above, the June 2021 outages of the Australian major banks' payment terminals and internet services were caused by issues with technology company Akamai's Prolexic software, which was providing a third party service to the major banks. This highlights the importance of ensuring the reliability of supply chains.
Personnel	Where critical personnel are immobilised for reasons that cannot be controlled, critical payment systems operations may be severely delayed or halted. Additionally, personnel with access to systems, data or	In 2018, a former personal banker at JP Morgan was sentenced to 48 months imprisonment for selling personal and account information that belonged to

[183] Crozier, 2021
[184] Fruhlinger, 2021
[185] RBA, 2018
[186] RBA, 2018

Risk	Identified Risk	Example
	premises may pose insider threat risks including fraud, theft, espionage, infrastructure sabotage and misuse of sensitive data.[187]	the bank's customers and using it himself to make unauthorised withdrawals from their accounts[188].
Physical & Natural	Increased occurrence of extreme weather events and natural disasters, including heatwaves, bushfires and floods, means physical payment systems infrastructure are experiencing heightened pressure. This stems from both increased demand for energy and the threat or realisation of damage to critical infrastructure, such as data centres. There is also a risk of sabotage by malicious actors to critical infrastructure's physical facilities. This could be used to disrupt the functioning of critical infrastructure and the systems which rely upon its function during times of heightened tension or conflict in the case of state-based actors.	As referenced above, in 2018, a power issue in NAB's mainframe in Melbourne caused extended outages across its internet, mobile banking, ATM and EFTPOS services. The outage resulted in consumers and small businesses being unable to process transactions on a busy trading day. NAB made $7.4M of compensation payments as a result of the outage[189].

[187] Ernst & Young, 2016

[188] United States Department of Justice, 2018

[189] Crozier, 2018

Existing legislation related to payment systems assets

Overview of regulation related to payment systems

Overview of regulation		Identified gaps
Payment Systems (Regulation) Act 1998	This Act provides for the regulation of payment systems and purchased payment facilities. The RBA has designated MasterCard, Visa, and EFTPOS to be payment systems, so they are governed by the Act. For the most part, the Act delegates the ability to regulate payment systems to the RBA, rather than laying out regulations itself. For example, section 18 gives the RBA the power to determine standards to be complied with by designated payment systems. However, the RBA's approach is to impose regulation only where (i) it considers it necessary in the public interest, and (ii) where the industry is unable or unwilling to address the RBA's concerns. As a result, the RBA has imposed relatively little regulation to cover only specific issues. By way of example, the RBA has not imposed any regulation dealing with fraud prevention in retail payment systems.	This Act only gives the RBA the ability to impose regulations; it does not impose any requirements on payment systems as responsible entities. It also does not impose obligations on entities for all hazards risk management, with notable gaps in regulation for managing high-priority risks for the sector such as fraud.
RBA Payment System Regulations	As discussed above, the Payment Systems (Regulation) Act 1998 allows the RBA to impose payment system regulations. The RBA has imposed relatively little regulation, preferring to allow the industry to self-regulate unless it is unwilling/unable to. The minimal regulation that the RBA has imposed can be found here. The regulations cover interchange fees and restrictions on merchants in card systems.	The RBA regulations do not impose any requirements relating to risk management, which the industry self-regulates.
e-Payments Code	The ePayments code is a voluntary code of practice that regulates electronic payments including ATM, EFTPOS, credit card transactions, online payments, internet and mobile banking, and BPAY. It is administered by ASIC. At a high level, the code addresses how payment systems entities interact with customers, e.g. requirements to provide consumers with terms and conditions, rules for determining who pays for unauthorised transactions, and regimes for recording mistaken internet payments.	The ePayments Code does not address risk management. It is also voluntary, and therefore does impose obligations on a whole-of-sector basis to ensure security and resilience across the sector.

Existing standards, guidelines and regulators for payment systems assets

Hazard domain	Organisation	Standards & guidelines
Cyber	Security Standards Council	**Payment Card Industry Data Security Standard**: a set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment
	National Institutes of Standards and Technology (NIST)	Cybersecurity Programs
	International Organization for Standardization (ISO)	**ISO 27001** provides requirements for information security management systems. **ISO 31000**
	European Central Bank	**CROE Framework:** international maturity assessment for cyber resilience for financial markets infrastructure **SIPS article 15:** operational security
	Bank for International Settlements	**Principles for Financial Markets Infrastructure (PFMI) Principle 17:** principle-based guidance for mitigating operational risk
	Australian Signals Directorate	**Information Security Manual:** outlines a cyber security framework that organisations can apply, using their risk management framework, to protect their information and systems from cyber threats
Physical	Security Standards Council	**Payment Card Industry Data Security Standard**
Supply Chain	Security Standards Council	**Payment Card Industry Data Security Standard**
	Bank for International Settlements	**PFMI Principle 17**
	APRA	**CPS234 and 231:** prudential standards in relation to supply chain management

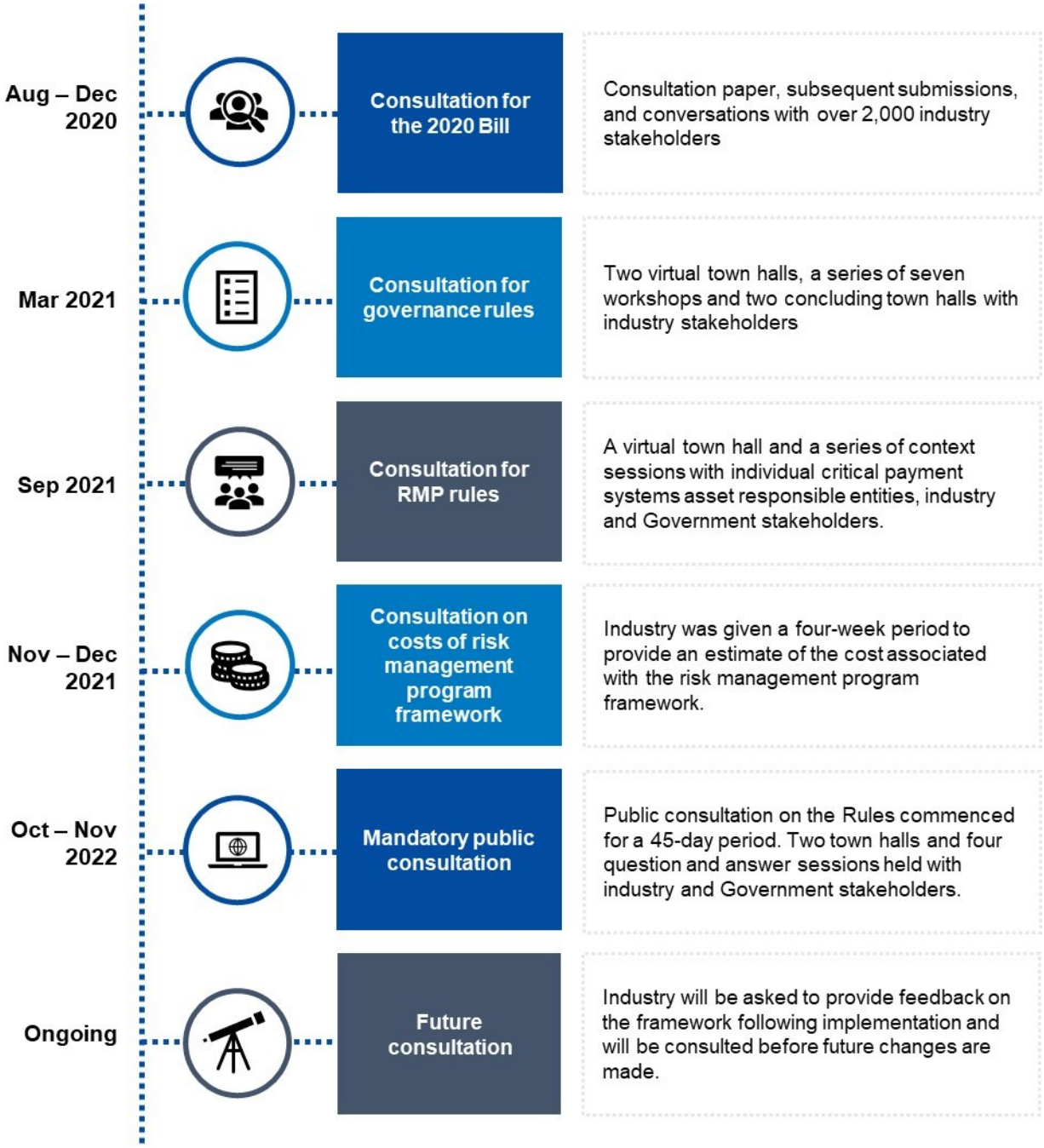
Jurisdiction	Regulator/s
Commonwealth	Reserve Bank of Australia

Additional information on consultation

Overview of stakeholders consulted

Stakeholders Consulted	
• Eftpos Payments Australia Limited	• Mastercard Inc.
• New Payments Platform Australia Limited	• Visa Inc.
• Reserve Bank of Australia	

Consultation timeline



RMP Rules consultation

The Department co-led the consultation with the Payment Systems Efficiency branch in the Policy Department of the Reserve Bank of Australia (RBA). This provided a detailed perspective on the sector's current regulatory obligations throughout consultation, with a view to avoiding regulatory overlap. Moreover, as the anticipated regulator for payment systems, the RBA's participation allowed for enhanced collaboration between Government and Industry.

Consultation with industry stakeholders occurred across the following key stages:

1. **A virtual briefing session**, held in September 2021 attended by approximately 10 industry and Government stakeholders, to communicate the purpose of the consultation process and obtain information to inform the design of future workshops.

2. **A series of virtual context sessions** held over a two-week period beginning in September 2021. These sessions were held between the Department and each of the responsible entities individually (Eftpos, Mastercard, NPPA and Visa) to allow for detailed and confidential discussion of the entity's unique operating and risk context. It provided a forum to consult on the RMP rules and assisted in understanding the costs and benefits associated with implementing the RMP framework. They also allowed the Department to understand responsible entities' commensurate regulatory obligations in other jurisdictions, to assist in avoiding regulatory overlap.
3. **Out of session consultation**, including meetings with a number of stakeholders and email communication.
   - Stakeholders were encouraged to contact the Department out of session. The Department availed itself to stakeholders to discuss their concerns, working to ensure stakeholders' understanding of the rules, and the rules' proportionality.
   - Out of session engagement also assisted in the iterative development of rules between the briefing session and context sessions, through addressing concerns raised by individual stakeholders and proposing a solution.
   - This engagement strengthened the relationship between the Department and industry, while providing insights on implementation costs, entities' operating environments and the overall impacts of the proposed regulatory changes.
4. **Two follow-up Information Sessions and two Industry-agnostic Town Halls** held in October and November 2021. The purpose of the information sessions was to provide an update for industry on the move from sector-specific to sector-agnostic RMP rules and to gain sector-specific feedback on the updated RMP rules. The purpose of the Industry Town Hall was to present the updated RMP rules and provide information on the further consultation period. The two information sessions were attended by approximately 17 and 18 industry and Government stakeholders respectively. The Town Hall was attended by approximately 800 industry and Government stakeholders across the 10 critical infrastructure sectors, including by stakeholders from the payment systems sector.
5. **Mandatory Public Consultation**, following the Minister commencing a 45-day consultation period on 5 October 2022 (the mandatory period is 28 days). Consultation included two Town Hall Sessions held on 10 October and 12 October 2022, attended by approximately 550 industry and Government stakeholders (across both sessions). The sessions provided information on the proposed RMP Rules as well as the broader obligation. These Town Halls, as well as four subsequent question and answer sessions, provided an opportunity for industry to ask questions about the proposed RMP Rules and process.

Key themes from consultation

Rule category	Identified themes		Impact on development of rules
Context to inform rules	**Context Sessions**	• Entities have high risk maturity. • Risk management processes are set up to ensure **consistent and reliable functioning** of payment systems for customers. • Common material risks across entities are **data breaches** and **fraud** • Global entities have **global risk management processes** and store data offshore. • Common standards implemented: NIST and ISO27001. • High reliance on telecoms and clearing banks.	In response to feedback received, the Department implemented: • Cybersecurity standards rules that allow for compliance with ISO 2700 • 1 and/or the NIST Cybersecurity framework. • Predominantly principles-based rules, in recognition that entities have sophisticated and, in many instances, global risk management processes. • Material risk rules that go towards ensuring the availability, reliability and integrity of critical infrastructure assets, in alignment with the priorities of industry.
Sector-agnostic RMP rules	**Information Sessions**	• Industry believes the RMP rules provide a baseline for sector resilience and security. • There is an appetite for guidance material to support sector-specific uplift in security and resilience. • Industry was seeking clarity on the definition of critical employees and whether it pertained to individuals (including contractors and sub-contractors) or roles.	In response to feedback received during the information sessions, the Department committed to: • The development of guidance materials, which would highlight aspects of risk management that should be prioritised by responsible entities and assist industry in interpreting and implementing the rules to achieve an uplift in security and resilience. • Changing the personnel hazards rules to refer to 'critical positions and/or critical personnel' rather than critical employees.

During the second information session, attendees were invited to participate in cost impact data collection through the completion of a cost impact template. This template was designed to collect substantive costing data to supplement the anecdotal costing discussions which had occurred throughout the workshop series. Industry were asked to provide:

- Their demographic information;
- Effort and cost estimates split by one-off and ongoing costs, staff effort, capital and other operating costs, and an estimated range between expected costs and highest possible costs; and
- Any comments on key boundaries, assumptions and cost drivers attached to the costing estimates provided.

Industry was provided with the template on 16 November 2021, with submissions open for a period of four weeks and closing on 14 December 2021.

The absence of entities within the sector that meet the definition of a small business indicated that consultation with the Australian Small Business and Family Enterprise Ombudsman was not required to identify expected costs to small businesses in preparing this RIS.[190]

[190] Office of Best Practice Regulation, 2021

Appendix M: Supplementary information for critical domain name systems assets

Overview of the role of domain name systems in Australia

As the Draft Critical Infrastructure Asset Definition Rules paper explains, the online environment is becoming increasingly intertwined with everyday life.[191] Use of the online environment is varied, from email communication, purchasing groceries and paying utility bills to facilitating significant business and financial transactions.

The Domain Name System is the internet's system for mapping alphabetic names (web addresses like 'cisc.gov.au') to numeric Internet Protocol addresses. This allows web users to download their desired webpage or file.[192]

The Australian '.au' namespace has over 3.2 million domain names registered as at August 2020.[193] Oversight of *.au* is provided by the .au Domain Administration (auDA), a not-for-profit organisation which operates under sponsorship from the Internet Corporation for Assigned Names and Numbers (ICANN) as well as endorsement from the Australian Government.[194] The Australian Government endorses auDA to administer the Australia's (*.au*) country code Top Level Domain (ccTLD) in accordance with the *Terms of Endorsement for auDA* (last updated in November 2021), published by the Department of Infrastructure, Transport, Regional Development and Communications.[195]

A disruption to this critical domain name system could have significant implications for Australian businesses, the government and the community, compromising users' ability to conduct business, navigate the internet, or access their data.

The SOCI Act refers to assets within a critical infrastructure sector as 'critical infrastructure assets'. Section 12KA of the SOCI Act, provides the following in relation to 'critical domain name systems':

An asset is a critical domain name system if it:

(a) is managed by an entity that, in accordance with subsection (2), is critical to the administration of an Australian domain name system; and

(b) is used in connection with the administration of an Australian domain name system;

(c) is an asset that, in accordance with subsection (3), is critical to the administration of an Australian domain name system.

Impacts of a disruption to critical domain name systems

- disruption to internet users' ability to conduct business and transactions, causing reduced economic activity;
- compromise of data security;
- inability of users to access their data; and
- inability of users to navigate to affected websites.

---

[191] Critical Infrastructure Centre, 2021, p. 21

[192] Oracle, n.d.

[193] Critical Infrastructure Centre, 2021, p. 21

[194] auDA, 2021

[195] Department of the Infrastructure, Transport, Regional Development and Communications, 2021

Examples of disruptions to critical domain name systems assets – domestic and international

DNS Hijacking[196]	Cyber
Situation: in 2019, a sophisticated hacker group called 'Sea Turtle' engaged in DNS hijacking, compromising multiple country-code top-level domains, including Armenia's .am top level domain.	
Outcome: Once the hackers gained full access to the domain registrar, they changed the target organisations' domain registration to point to their own DNS servers, instead of the targets' legitimate servers. When users attempted to reach the targets' network (through web, email etc.), the malicious DNS servers redirected the traffic to different 'man-in-the-middle' servers that intercepted and spied on all the communications before passing them on to their intended destination. Through this technique, the hackers harvested usernames and passwords from the intercepted traffic. It is believed that the hackers targeted governmental organisations, including intelligence agencies, ministries of foreign affairs, and energy related groups.	
Identified Gap: This type of attack could have been prevented by use of SSL certificates, that assure that the recipient of encrypted internet traffic is who it claims to be.	

DNS Outage brings down many popular websites[197]	Supply Chain
Situation: Multiple popular websites became temporarily unavailable in July 2021, following a DNS outage at Akamai, an internet services company which provides networking and content delivery services to many companies. The affected websites included those of HSBC, Barclays, British Airways, Morgan Stanley, Airbnb, UPS and FedEx, causing significant disruption to commercial activity.	
Outcome: The outage was triggered by a bug in the DNS system caused by a system update. Upon rolling back the software update, the bug was resolved, and the affected websites resumed normal operations. The outage lasted approximately an hour. Through this case study, we can see how DNS outages can have a cascading effect on other critical infrastructure assets. Here, the DNS outage affected the availability of online banking (several large Australian banks will be named critical banking assets), and critical freight services. It is easy to picture a scenario where DNS outages could cause disruption to other critical infrastructure assets. For example, DNS outages could affect the availability of online financial services, and online grocery shopping which are particularly important in situations such as COVID-19 lockdowns.	
Identified Gap: This case study demonstrates the importance of ensuring the reliability of service providers such as Akamai, whose outages may have significant on effects.	

Key risks to critical domain name systems assets

Hazard domain	Identified risk	Example
Cyber	Domain name systems operate in the digital world, so cyber threats are particularly important to manage. Cyber threats may cause significant disruption to DNS systems, causing downtime for websites, and	As referenced above, in 2019 a sophisticated group of hackers called Sea Turtle engaged in DNS hijacking, compromising multiple cc TLDs. The hackers were able to harvest usernames

[196] Greenberg, 2019

[197] Whittaker, 2021

	compromising data security.	and passwords, including that of users from government agencies. [198]
Supply Chain	The communications sector relies on international cooperation and other services to function for services such as internet access. While the stability of this sectors' suppliers may be relevant due ongoing services, many of the other critical functions that support Australians are not significantly threatened by this vector.	As referenced above, In July 2021, multiple popular websites became temporarily unavailable due to a DNS outage at an internet services company. This example reinforces the need to ensure the reliability of service providers within the supply chain. [199]
Personnel	The ongoing availability of DNS services may be dependent on the availability of critical personnel. Where these personnel are not available, critical DNS operations may be severely delayed or halted. Additionally, personnel with access to systems, data or premises may pose insider threat risks, including infrastructure sabotage, and misuse of sensitive data.	While there are no specific examples of malicious insiders in organisations operating domain name systems, examples can be found in related industries. For example, Verizon's 2019 Insider Threat Report identified that 57% of database breaches involved insider threats.[200]
Physical and Natural	DNS services are highly reliant on the communications network, including telecommunications infrastructure such as fibre optic cables and satellite dishes. It is also highly reliant on energy. As a result, physical and natural risks to this infrastructure (e.g. natural disasters, terrorist attacks) pose a threat to the ongoing availability of critical domain name system services.	In 2011, an underwater cable that links south-east Asia to Europe was cut, causing internet interruptions to the Middle East and South Asia.[201]

Existing legislation related to critical domain name systems assets

Overview of regulation		Identified gaps
Telecommunications Act 1997	The Telecommunications Act 1997 seeks to provide a regulatory framework in relation to carriage services. Carriage services are defined as services for carrying communications by means of guided and/or unguided electromagnetic energy. The Telecommunications Act (sections 474-477) does also provide ACMA and the ACCC with the power to give directions to a 'declared manager of electronic addressing'; this essentially gives the government reserve power to regulate with respect to domain names, although in practice the government has endorsed auDA to manage the operation of the .au domain space.	The Telecommunications Act provides the government with reserve powers to regulate in relation to domain names but does not specifically address risk management.
Australian	Sections 11 and 17 of the Australian	The Australian

[198] Greenberg, 2019
[199] Whittaker, 2021
[200] Kohen, 2019
[201] Yahoo News, 2011

Communications and Media Authority Act 2005	Communications and Media Authority Act 2005 give ACMA the reserve power to 'provide for the management of electronic addressing' if instructed to do so by the minister; this essentially gives the government reserve power to regulate with respect to domain names, although in practice the government has endorsed auDA to manage the operation of the .au domain space.	Communications and Media Authority Act 2005 provides the government with reserve powers to regulate in relation to domain names but does not specifically address risk management.
Telecommunications and Other Legislation Amendment Act 2017	The Telecommunications and Other Legislation Amendment Act 2017 amended the Telecommunications Act 1997, adding extra provisions that place greater security obligations on carriers and carriage service providers.	This Act and its provisions do not apply to auDA as it is not a carrier or carriage service provider.
Terms of Endorsement (ToE) for auDA	While not legislation, these terms set the Government's expectations for auDA. They state that the Australian Government endorses the .au Domain Administration (auDA) to administer Australia's (.au) country code Top Level Domain (ccTLD) contingent on auDA continuing to meet the conditions of endorsement. These include responding quickly to matters that compromise the security and integrity of the Domain Name System (DNS) and maintaining appropriate security protocols in line with Australian and international best practice, and contemporary security practices.	Though the ToE create contractual obligations between the Government and auDA, they do not create regulatory obligations for compliance. They also do not set specific baseline security standards.

Existing standards, guidelines and regulators for critical payment systems assets

Hazard domain	Organisation	Standards & guidelines
Cyber	Australian Cyber Security Centre (ACSC)	**Cyber Security Guidelines, Information Security Manual, Essential Eight Maturity Model**
	Australian Signals Directorate	**Information Security Manual**
	ACSC	**Information Security Manual (ISM)**
	NIST	**SP 800-81-2: Secure Domain Name System (DNS) Deployment Guide:** presents guidelines for configuring DNS deployments to prevent many denial-of-service attacks that exploit vulnerabilities in various DNS components.
Physical	ISO	**ISO 55001**
Personnel	Standards Australia	**AS 4811-2006**
Supply Chain	APRA	**CPS 231, 234**
	Australian Cyber Security Centre	**Supply Chain Guidance for Practitioners**
	ICANN	**Framework for Registry Operators to Respond to Security Threats**: This framework is a voluntary and non-binding document designed to articulate the ways registries may respond to identified security threats. This is relevant for supply chain threats because the AuDA outsources their registry operation function.

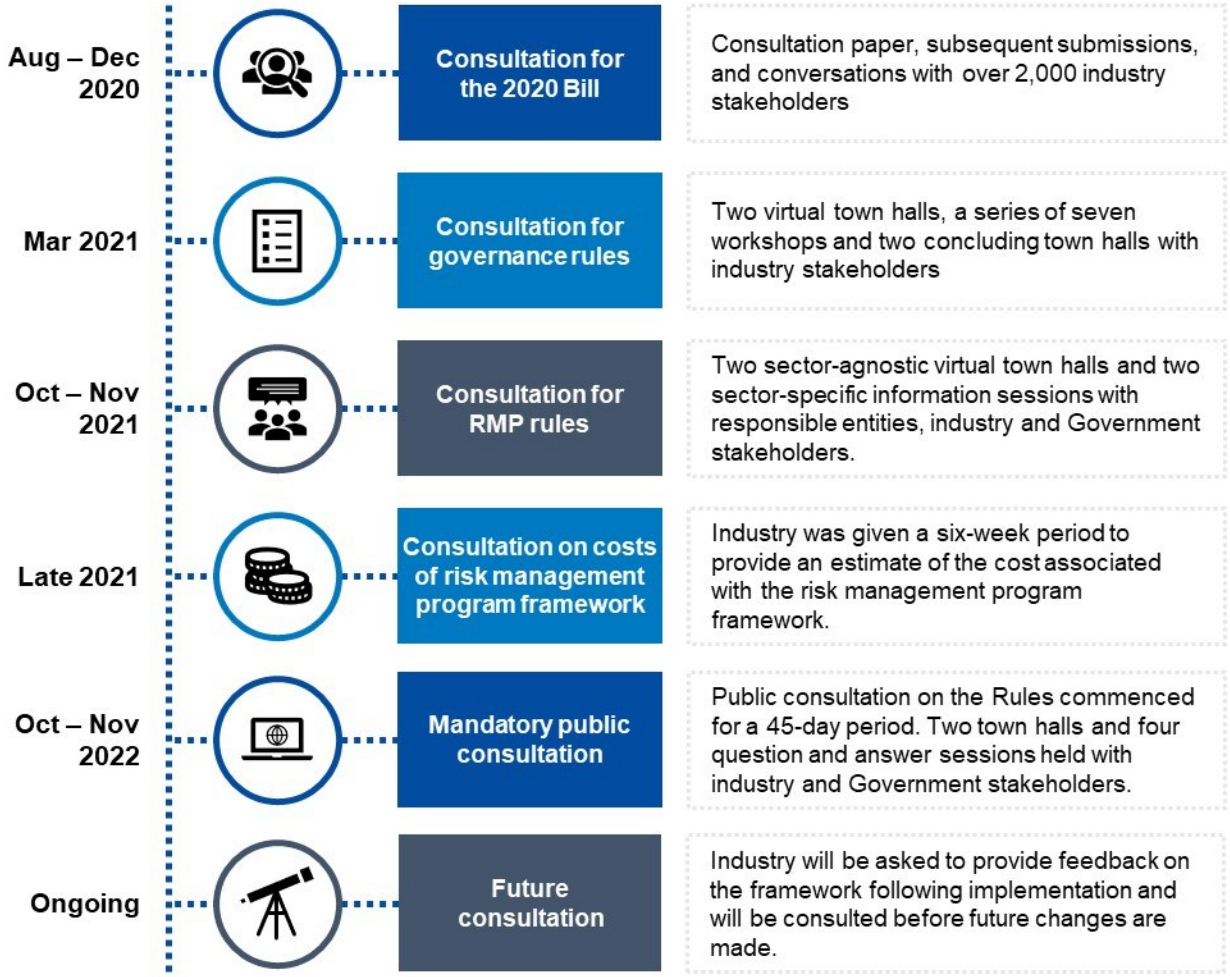
Jurisdiction	Regulator/s
Commonwealth	auDA Australian Communications and Media Authority (through reserve powers as per Telecommunications Act 1997, sections 474-477 and Australian Communications and Media Authority Act 2005, sections 11 and 17) Australian Competition & Consumer Commission (through reserve powers as per Telecommunications Act 1997, sections 474-477) ccTLD Sponsorship Agreement (.au): Agreement between Internet Corporation for Assigned Names and Numbers (ICANN) and auDA stating that ICANN will sponsor auDA as the administrator of the .au top level-domain, with ICANN continuing to preserve the technical stability and operation of the DNS.

Additional information on consultation

Overview of stakeholders consulted

Stakeholders Consulted
auDA

Consultation timeline



RMP Rules consultation

Consultation with industry stakeholders occurred across the following key stages:

1. **A virtual Town Hall**, held on 19 October 2021, attended by 360 approximately industry and Government stakeholders, including from the domain name systems sector. The purposes of the session were to:
   i. Outline the CI/SONS reforms and provide an update on the SLACI Bill (now SLACI Act) and SLACIP Bill (now SLACIP Act);
   ii. Provide an update for industry on the decision to consult on sector-agnostic RMP rules (as opposed to sector-specific rules), and outline how this would affect the consultation process going forward; and
   iii. Answer any questions about the Bills or RMP rules consultation process.
2. **Two domain name systems-specific Information Sessions,** held on 11 November and 23 November 2021, attended by approximately eight industry and Government stakeholders. The purpose of the information sessions was to reiterate the update for industry on the move from sector-specific to sector-agnostic RMP rules and to gain sector-specific feedback on the RMP rules.
3. **A wrap-up virtual Town Hall** held on 25 November 2021. The purpose of the Town Hall was to present the updated RMP rules and provide information on the further consultation period. The Town Hall was attended by approximately 800 industry and Government stakeholders across the 10 critical infrastructure sectors, including by stakeholders from the domain name systems sector.
4. **Out of session consultation:**
   – Stakeholders were encouraged to contact the Department out of session. The Department availed itself to stakeholders to discuss their concerns, working to ensure stakeholders' understanding of the rules, and the rules' proportionality.
   – Out of session engagement also assisted in the iterative development of rules between workshops, through addressing concerns raised by individual stakeholders and proposing a solution.
   – This engagement strengthened the relationship between the Department and industry, while providing insights on implementation costs, entities' operating environments and the overall impacts of the proposed regulatory changes.
5. **Mandatory Public Consultation**, following the Minister commencing a 45-day consultation period on 5 October 2022 (the mandatory period is 28 days). Consultation included two Town Hall Sessions held on 10 October and 12 October 2022, attended by approximately 550 industry and Government stakeholders (across both sessions). The sessions provided information on the proposed RMP Rules as well as the broader obligation. These Town Halls, as well as four subsequent question and answer sessions, provided an opportunity for industry to ask questions about the proposed RMP Rules and process.

Outcomes and themes from consultation on RMP rules

Key themes from consultation

Rule category	Identified themes	Impact on development of rules

Rule category	Identified themes		Impact on development of rules
RMP rules	**Information sessions**	• The domain names systems sector **broadly agrees** with the RMP rules as drafted. • There is an **appetite for guidance material** to support sector-specific uplift in security and resilience. Industry was receptive to supporting Government to devise this material. • Industry welcomed the use of **AusCheck.**	In response to feedback received during the information sessions, the Department committed to the development of guidance materials, which would highlight aspects of risk management that should be prioritised by responsible entities and assist industry in interpreting and implementing the rules to achieve an uplift in security and resilience.

Consultation on costs

During the second information session, attendees were invited to participate in cost impact data collection through the completion of a cost impact template. This template was designed to collect substantive costing data to supplement the anecdotal costing discussions which had occurred throughout the workshop series. Industry were asked to provide:

- Their demographic information;
- Effort and cost estimates split by one-off and ongoing costs, staff effort, capital and other operating costs, and an estimated range between expected costs and highest possible costs; and
- Any comments on key boundaries, assumptions and cost drivers attached to the costing estimates provided.

Industry was provided with the template on 24 November 2021, with submissions open for a period of four weeks and closing on 22 December 2021.

The absence of entities within the sector that meet the definition of a small business indicated that consultation with the Australian Small Business and Family Enterprise Ombudsman was not required to identify expected costs to small businesses in preparing this RIS.[202]

[202] Office of Best Regulation Practice, 2021

Appendix N: Supplementary information for critical liquid fuels assets

Overview of the role of liquid fuels in Australia

Australia's economy is reliant on liquid fuel and will be for some time to come. Liquid fuel makes up 52 per cent of Australia's final energy consumption and includes petrol, diesel, jet fuel and biofuels. Our demand is different depending on fuel type. Diesel demand is growing faster than the economy, driven by growth in mining and agriculture and growth in diesel vehicle use. The fast-growing market for international tourism to Australia is also pushing up jet fuel demand. Petrol use has levelled off as people switch to diesel-fuelled cars, and fuel efficiencies in petrol vehicles allow people to drive further on each litre of fuel.[203]

The transport sector makes up 75 per cent of our total liquid fuel demand. It includes road (passenger and freight), rail, shipping and air transport. Mining, agriculture and manufacturing (including petrochemicals) make up the most significant industry demand for liquid fuel. Both mining and agriculture are over 90 per cent reliant on diesel, and this partly drives the growth in demand for diesel. Under normal circumstances, use by the Australian Defence Force equates to three per cent of our national demand for jet fuel and about 0.5 per cent of national demand for diesel. This suggests that any actions taken to improve fuel security in Australia need to take into consideration fuel types and usage. Securing diesel and jet fuel is more important than securing supplies of petrol. In an emergency, we are most likely to need diesel and jet fuel for essential users. However, we know that Australia holds less stock and meets less of our own refining needs for diesel when compared with petrol.[204]

The SOCI Act refers to assets within a critical infrastructure sector as 'critical infrastructure assets'. Section 12A of the SOCI Act by provides the following in relation to 'critical liquid fuels assets':

*(1) An asset is a **critical liquid fuels asset** if it is:*

(a) A liquid fuel refinery that is critical to ensuring the security and reliability of a liquid fuel market, in accordance with subsection (2); or

(b) A liquid fuel pipeline that is critical to ensuring the security and reliability of a liquid fuel market, in accordance with subsection (3); or

(c) a liquid fuel storage facility that is critical to ensuring the security and reliability of a liquid fuel market, in accordance with subsection (4).

(2) For the purposes of paragraph (1) (a), the rules may prescribe: (a) specified liquid fuel refineries that are critical to ensuring the security and reliability of a liquid fuel market; (b) requirements for a liquid fuel refinery to be critical to ensuring the security and reliability of a liquid fuel market.

(3) For the purposes of paragraph (1)(b), the rules may prescribe: (a) specified liquid fuel pipelines that are critical to ensuring the security and reliability of a liquid fuel market; or (b) requirements for a liquid fuel pipeline to be critical to ensuring the security and reliability of a liquid fuel market.

[203] Liquid Fuel Security Review

[204] Ibid

(4) For the purposes of paragraph (1)(c), the rules may prescribe: (a) specified liquid fuel storage facilities that are critical to ensuring the security and reliability of a liquid fuel market; or (b) requirements for a liquid fuel storage facility to be critical to ensuring the security and reliability of a liquid fuel market.

Impacts of a disruption to critical liquid fuel assets

- Disruptions to transport infrastructure, traffic management systems and fuel supplies;
- Reductions in the reliability of the supply of food and groceries, in particular relating to the agriculture sector;
- Disruptions to Australia's defence capabilities; and
- An inability for businesses and governments to function as normal.

Examples of disruptions to critical liquid fuel assets – domestic and international

2021 United Kingdom (UK) Fuel Supply Crisis	Supply chain, personnel
Situation: In September 2021, the UK suffered a fuel supply shortage for a period of a few weeks, in which petrol stations in some parts of the UK ran out of fuel completely. There were lengthy line-ups at petrol stations and panic buying occurred, putting supply chains under extreme pressure. A £30 ($54 AUD) cap on fuel purchases was imposed to help manage the limited fuel supply.[205]	
Outcome: The fuel supply crisis impacted businesses who rely on fuel to fill up their car to run their services and earn their income, especially for taxi drivers. As a result of the shortage and the surge in demand, several petrol stations increased their rates. There was also a rapid depletion of fuel supplies and a labour shortage in critical industries such as road transportation, processing and handling, distribution, and manufacturing.[206]	
Identified Gap: According to industry experts, the fuel supply crisis was caused by a variety of factors, including a shortage of Heavy Goods Vehicle (HGV) drivers, leaked information about BP storage levels, Brexit, and the COVID-19 pandemic. The truck shortage impacted the British economy significantly, as HGV drivers were faced with delays in obtaining their licences due to the COVID-19 pandemic. Salary increases for HGV drivers had also been implemented to retain the number of drivers in the workforce and to ensure that there are adequate drivers available to drop of supplies. Overall, the event demonstrated the need for improved regulations and advanced contingency planning to reduce the levels of disruptions in the future.[207]	

2010 Great Barrier Reef Oil Spill	Natural Hazard, Physical
Situation: On 3 April 2010, a massive oil spill occurred in Central Queensland, Australia's Great Barrier Reef. The bulk coal carrier MV Shen Neng 1 travelled east of Rockhampton, more than ten kilometres outside the shipping route, and caused the reef's longest grounding heavy liquid fuel oil scar. The scar was approximately three kilometres long and had caused significant long-term damage to the reef.[208]	

[205] Taylor, 2021
[206] Bloomberg, 2021
[207] Cotton, 2021
[208] McKinnell, Lu, 2016

Outcome: The oil spill clean-up cost $141 million dollars, and the owner of the Chinese coal ship that went around the Great Barrier Reef agreed to pay the Queensland government $35 million dollars and the Great Barrier Reef Marine Park Authority $4.3 million dollars (GBRMPA). Additionally, the spill had a significant environmental impact, as it killed approximately 400 kinds of animals and 500 types of plants. Certain regions have been completely devoid of marine life, resulting in significant long-term harm to the reef.[209]

Identified Gap: The Australian Transport Safety Bureau launched an enquiry and issued a preliminary report concluding that the officer on duty was fatigued and failed to programme a proposed course adjustment into the ship's GPS navigation system. Additionally, the investigation showed that the chief officer failed to draw the ship's location on the nautical chart at intervals that were suitable. As a result, the ship's system and infrastructure failed to offer notice and there were no properly trained officials on board. The event reflects the need for appropriate infrastructure requirements to prevent emergency disasters like the reef oil spill.[210]

Tehran Fuel Stations Cyber Attack	Cyber security

Situation: In October 2021, Iran's fuel distribution system was brought to a halt following an unprecedented cyber-attack suspected to have been launched from abroad. The cyber-attack disrupted the country's electronic card system, which motorists use to purchase substantially subsidised fuel and hours long lines were formed during the crisis.[211]

Outcome: Anyone that was attempting to purchase fuel via the machines using a government-issued card instead saw a notice saying "cyber-attack 64411." The majority of Iranians rely on these subsidies to fuel their automobiles, especially in light of the country's economic difficulties. The failure of the intelligent fuel system resulted in the inability of the system to identify the fuel cards, as many fuel stations only sell fuel via this method.[212]

Identified Gap: Iran has been subjected to a series of cyber-attacks, and while the nation has disconnected much of its government infrastructure from international access, the infrastructure, legislation, and regulations do not have enough protections against this type of disconnection and cyber-attacks, highlight the need for appropriate measures in place to prevent future attacks in future.[213]

Colonial Pipeline Cyber Attack	Cyber security

Situation: On May 7, 2021, the Colonial Pipeline, which is the largest pipeline in the American oil pipeline system and mostly transports oil and jet fuel to the south-east of United States, was hit by the largest ransomware cyber-attack in the history of the liquid fuels industry The attack affected the pipeline's computerised equipment and forced some airlines to make fuel stops on long-haul flights. The attack provoked the shutdown of the pipeline operations for a total of five days and also resulted in temporary fuel shortage along the East Coast.[214] The ransomware attack was a form of malware that encrypts data until the victim pays and threatens to release the data online.

Outcome: This attack brought the pipeline's operations to a stop, and on the fourth day of the attack, fuel shortages began at filling stations and panic buying occurred across Alabama, Florida, Georgia, North Carolina, and South Carolina. Additionally, average gasoline prices increased to their highest level since 2014, surpassing $3 per gallon. The Colonial Pipeline made the ransom payment to the hacking group, roughly of a total of $5 million USD ($6.49 million AUD) to restore the system and recover its stolen data. [215]

[209] Ibid
[210] Moore, 2016
[211] 7 News, 2011
[212] Times of Israel, 2021
[213] Ibid
[214] ABC News, 2021
[215] Ibid

Identified Gap: The cybersecurity specialists confirmed that the breach occurred as a consequence of a single compromised password. The hackers got access to the colonial pipeline's network using a virtual private network account that permitted employees to access the company's computer network remotely. The attack demonstrated the need of fuel industries and systems to keep up with increasing malware capabilities and work to improve the economy's security to fuel operations.[216] Without adequate safeguards and continuous re-evaluation, important operational systems for mitigating catastrophic occurrences will continue to be threatened.

Key risks to critical liquid fuels assets

Hazard domain	Identified risk	Example
Physical	Increased occurrence of extreme weather events and natural disasters, including heatwaves, bushfires and floods, means liquid fuels infrastructure is experiencing heightened pressure. This stems the threat or realisation of damage to critical infrastructure, oil pipelines.	In July 2021, a fire on the ocean surface west of Mexico's Yucatan peninsula was extinguished, which was due to the gas leak from an underwater pipeline that connects to a platform at Pemex's flagship Ku Maloob Zaap oil development. Pemex, which has a long record of major industrial accidents at its facilities, also shut the valves of the 12-inch-diameter pipeline. [217]
Cyber	Cyber-attacks in the oil and gas industry can threaten an organisation's information technology (IT), its operational technology (OT) and any internet of things (IoT) systems in place. A breach in industrial control systems could cause a serious occupational health and safety event, which in an industry focused on creating zero harm work environments, could cause serious harm to an individual and an organisation's ability to operate.	A cyberattack forced the temporary shutdown of the one of the US's largest pipelines, the Colonial pipeline, highlighting concerns over the vulnerabilities in the US's critical infrastructure. Colonial, which transports more than 100 million litres and daily from Houston to the New York Harbor. In response to the attack, certain systems had to be turned offline to contain the threat, which halted all pipeline operations and affected some of the IT systems. [218]
Supply Chain	Disruption to supply chains pertinent to critical liquid fuel assets may have detrimental consequences. Australia is heavily reliant on commercial stock of crude oil and refined products to maintain fuel supplied. The recent closure of Australian refineries will increase our reliance on imports under both normal conditions and during a liquid fuel emergency.[219]	In Australia, there has been shortages of special anti-pollution additive for diesel vehicles (AdBlue), which is placing further pressures on an already strained supply chain. Should the shortages continue, it is anticipated there will be a cascading impact across the country, also affecting the agricultural and power sectors, which rely heavily on diesel motors.[220]
Personnel	Where personnel are immobilised for reasons that cannot be controlled, critical liquid fuels operations may be severely delayed or halted. Additionally, personnel with access to systems, data or premises may pose insider threat risks	The COVID-19 pandemic saw key industry personnel subject to extended periods of quarantine, forcing the closure of some liquid fuels generators or reduced capacity where insufficient personnel were available.

[216] Bloomberg, 2021
[217] Barrera, 2021
[218] Stracqualursi, 2021
[219] OBPR, 2021
[220] Ferguson, 2021

Hazard domain	Identified risk	Example
	including fraud, theft, espionage, infrastructure sabotage and misuse of sensitive data.[221]	

Existing legislation related to critical liquid fuel assets

Overview of regulation		Identified gaps
Fuel Security Act 2021 (Cth)	Establishes a minimum stockholding obligation for corporate entities that undertake certain activities (broadly, importing and refining) in relation to certain transport fuels to hold a minimum quantity of those fuels nationally; and enable a production payment for refinery operators (referred to as a fuel security services payment) to provide an adjustable cent per litre payment to refineries in return for a commitment to continue refining until at least 30 June 2027.	While the Act is pushing for sovereign capability to protect fuel dependent industries and fuel disruptions, it does not have an all-hazards approach to secure recovery from disruptions and an emergency contingency plan.
Liquid Fuel Emergency Act 1984 (Cth)	In the event of an actual or likely fuel shortage with national implications, the Governor General may declare a national liquid fuel emergency under this Act. The Act gives the Minister for Department of Climate Change, Energy, the Environment and Water powers in an emergency to control: Industry-held stocks of crude oil and liquid fuels; production by Australian refineries; and fuel sales across Australia.	While the risk management element contained in these legislative regimes may contribute to suitable risk management, they do not amount to an all-hazards approach to risk management, nor are security risk management obligations imposed on a whole-of-sector basis.
Liquid Fuel Emergency Amendment Act 2017 (Cth)	The Act enables the Australian Government to enter into commercial oil stockholding contracts with Australian and foreign entities.	While the Act has some risk management features in the sections relating to the emergency supply of liquid fuels, it does not cover a risk management approach of foreign entities. There is a lack of requirements to reduce cyber security, supply-chain and personnel hazards in the Act.
The Pipelines Act 2005 (VIC)	The primary Act governing the construction and operation of pipelines carrying liquid and gaseous fuels at high pressure in Victoria. The Acts covers 'high transmission' pipelines that have maximum design pressure exceeding 1050 kPa for gaseous hydrocarbons and 345 kPa for liquids.	While Victoria has never suffered a large-scale pipeline incident, there is a lack of requirements to reduce cyber security, supply-chain and personnel hazards in the Act. As it is evident that third party interference with pipeline remains one of the biggest threats to pipeline safety, the Act does not have a risk management approach to foreign interference and potential of serious disruptions.
Pipelines Act 1967 (NSW)	The Act covers the structure for protecting or supporting a pipeline, storage tanks, loading	There is a lack of requirements to reduce cyber security, supply chain and personnel

[221] Ernst & Young, 2016

Overview of regulation		Identified gaps
	terminals and works and buildings used or to be used for purposes connect with or incidental to the operation of a pipeline. The Act also monitors the compliance, allocation and requirement of pipeline licences.	hazards in the Act. As it is evident that third party interference with pipeline remains one of the biggest threats to pipeline safety, and the Act does not have a risk management and hazard security risk approach to prevent the interference's from cyber criminals and disruptions.
Liquid Fuel Supply Act 1984 (QLD)	This Act requires fuel sellers (fuel retailers and fuel wholesalers) to sell minimum amounts of sustainable bio-based fuel.	While the Act holds retailers accountable for mandated reporting, it lacks criteria for an all-hazards approach to transportation and protection in the event of a liquid fuel interruption. Additionally, there is no plan for avoiding future supply chain disruptions through, for example, cyber-attacks.
Liquid Fuel Supply Regulation 2016 (QLD)	Sets sustainability criteria for biofuels sold under Queensland's biofuels mandate. Fuel sellers (retailers and wholesalers) who are liable to meet the mandate need to report volumes of sustainable bio-based petrol and sustainable bio-based diesel under section 35E of the Act.	Under the Liquid Fuel Supply Act 1984, it lacks criteria for an all-hazards approach to transportation and protection in the event of a liquid fuel interruption. Additionally, there is no plan for avoiding future supply chain disruptions through, for example, cyber-attacks.
Fuel, Energy and Power Resources Act 1972 (WA)	The Act provides conservation and efficient use of current and future sources and supplies of fuel, energy, and power in and to Western Australia, as well as the establishment and functions of the Western Australian Fuel and Power Commission and the Fuel and Power Advisory Council, and for other purposes.	While the Act has some risk management features in the sections relating to the management of liquid fuel supply, and has requirements to reduce the risk of specific hazards, it does not amount to an all hazards approach to risk management. There is a lack of requirements to reduce cyber security, supply-chain and personnel hazards in the Act.
Offshore Petroleum and Greenhouse Gas Storage Act 2006 (Cth	The Offshore Petroleum and Greenhouse Gas Storage Act 2006 (OPGGS Act) and associated regulations provides the legal framework for the exploration and recovery of petroleum and greenhouse gas activities in Commonwealth waters (those areas that are more than three nautical miles from the territorial seal baseline).	While the Act effectively has a framework to monitor and enforce compliance to prevent accidents and occurrences of petroleum and gas to the environment and waters, they do not amount to an all-hazards approach to risk management, nor are risk management obligations imposed on a whole-of-sector basis.
Fuels Rationing Act 2019 (ACT)	The powers provided under the Act may be used by the Minister in the event or likely event that a shortage of liquid fuel supplies is severe enough that normal industry processes, fuel stored, alternative supplies, and price fluctuations could not alone guarantee sufficient supply.	While the Act provides the ability to manage and respond to a potential liquid fuel shortage, it does not amount to risk management and all hazards security risk management approach.
Fuel Quality Standards Regulations 2019	The regulations aim to provide the administrative detail for the following matters: application processes for an approval to vary a fuel standard; · appointment conditions of the Fuel Standards Consultative Committee; · publication of notices of action in relation to adding or removing a fuel additive, or class of fuel additive.	While the regulation provides the administrative requirement for fuel quality regulations, it does not amount to an all-hazards approach to risk management, nor is the requirement for a safety management scheme imposed on a whole-of-sector basis.

Existing standards, guidelines and regulators for critical liquid fuel assets

Hazard domain	Organisation	Standards & guidelines
Cyber	National Institutes of Standards and Technology (NIST)	**Cybersecurity Programs**
	International Organization for Standardization (ISO)	**ISO 27001** provides requirements for information security management systems.
	United States Department of Energy	**Cybersecurity Capability Maturity Model** (C2M2) was developed by the U.S. Department of Energy in conjunction with energy sector subject matter experts. It provides a voluntary evaluation process which allows entities to determine the maturity of their cyber security capabilities. The AESCSF is based upon this model.
	ACSC	**Essential Eight Maturity Model** provides requirements to increase business resilience against cyber and information security hazards.

Jurisdiction	Regulator/s
Commonwealth	Department of Climate Change, Energy, the Environment and Water Fuel Quality Standards Regulations 2019
Australian Capital Territory	ACT Fair Trading
New South Wales	NSW Fair Trading
Northern Territory	NT Consumer Affairs
Queensland	QLD Office of Fair Trading
South Australia	SA Consumer Complaints and Advice
Tasmania	Consumer Affairs and Fair-Trading Tasmania
Victoria	Agriculture Victoria Consumer Affairs Victoria
Western Australia	WA Consumer Protection

Additional information on consultation

Overview of stakeholders consulted

Stakeholders Consulted	
• Santos • Ampol • Chevron • Viva Energy	• The National Offshore Petroleum Safety and Environmental Management Authority (NOPSEMA) • Woodside Energy • The Australian Petroleum Production & Exploration Association (APPEA)

RMP Rules consultation

Consultation with industry stakeholders occurred across the following key stages:

1. **A virtual Town Hall**, held on 19 October 2021, attended by approximately 360 industry and Government stakeholders, including from the liquid fuels sector. The purposes of the session were to:
    i. Outline the CI/SONS reforms and provide an update on the SLACI Bill (now SLACI Act) and SLACIP Bill (now SLACIP Act);
    ii. Provide an update for industry on the decision to consult on sector-agnostic RMP rules (as opposed to sector-specific rules), and outline how this would affect the consultation process going forward; and
    iii. Answer any questions about the Bills or RMP rules consultation process.
2. **Two liquid fuels-specific Information Sessions,** held on 10 November and 22 November 2021, attended by approximately 50 and 30 industry and Government stakeholders respectively. The purpose of the information sessions was to reiterate the update for industry on the move from sector-specific to sector-agnostic RMP rules and to gain sector-specific feedback on the RMP rules.
3. **A wrap-up virtual Town Hall** held on 25 November 2021. The purpose of the Town Hall was to present the updated RMP rules and provide information on the further consultation period. The Town Hall was attended by approximately 800 industry and Government stakeholders across the 10 critical infrastructure sectors, including by stakeholders from the liquid fuels sector.
4. **Out of session consultation:**
    – Stakeholders were encouraged to contact the Department out of session. The Department availed itself to stakeholders to discuss their concerns, working to ensure stakeholders' understanding of the rules, and the rules' proportionality.
    – Out of session engagement also assisted in the iterative development of rules between workshops, through addressing concerns raised by individual stakeholders and proposing a solution.
    – This engagement strengthened the relationship between the Department and industry, while providing insights on implementation costs, entities' operating environments and the overall impacts of the proposed regulatory changes.
5. **Mandatory Public Consultation**, following the Minister commencing a 45-day consultation period on 5 October 2022 (the mandatory period is 28 days). Consultation included two Town Hall Sessions held on 10 October and 12 October 2022, attended by approximately 550 industry and Government stakeholders (across both sessions). The sessions provided information on the proposed RMP Rules as well as the broader obligation. These Town Halls, as well as four subsequent question and answer sessions, provided an opportunity for industry to ask questions about the proposed RMP Rules and process.

Outcomes and themes from consultation on RMP rules

Key themes from consultation

Rule category	Identified themes	Impact on development of rules
RMP rules	**Information sessions** • The liquid fuels sector **broadly agrees** with the RMP rules as drafted. • The sector expressed a desire to **avoid regulatory duplication.** • There is an **appetite for**	In response to feedback received during the information sessions, the Department committed to: • Allowing responsible entities to leverage existing reporting requirements where appropriate, reflecting this in the rules and guidance material; and

Rule category	Identified themes	Impact on development of rules
	guidance material to support sector-specific uplift in security and resilience. For example, around defining 'equivalent' standards and background checks to AusCheck.	• The development of guidance materials, which would highlight aspects of risk management that should be prioritised by responsible entities and assist industry in interpreting and implementing the rules to achieve an uplift in security and resilience.

Consultation on costs

During the second information session, attendees were invited to participate in cost impact data collection through the completion of a cost impact template. This template was designed to collect substantive costing data to supplement the anecdotal costing discussions which had occurred throughout the workshop series. Industry were asked to provide:

- Their demographic information;
- Effort and cost estimates split by one-off and ongoing costs, staff effort, capital and other operating costs, and an estimated range between expected costs and highest possible costs; and
- Any comments on key boundaries, assumptions and cost drivers attached to the costing estimates provided.

Industry was provided with the template on 22 November 2021, with submissions open for a period of four weeks and closing on 20 December 2021.

The absence of entities within the sector that meet the definition of a small business indicated that consultation with the Australian Small Business and Family Enterprise Ombudsman was not required to identify expected costs to small businesses in preparing this RIS.[222]

[222] Office of Best Regulation Practice, 2021

Appendix O: Supplementary information for critical hospital assets

Overview of the role of critical hospitals in Australia

Hospitals are an important part of Australia's health care system. In Australia, public hospitals are largely owned and managed by State and Territory Governments, and private hospitals are owned and managed by private for-profit and not-for-profit organisations. All hospitals can receive funding from Governments, individuals, and insurers. Intensive care units (ICUs) are one of the most critically functioning operational environments in a hospital. Every ICU in a hospital has a different environment that will reflect the specialist medical and surgical procedures they perform. Most ICUs are large, sterile areas with a high concentration of specialised, technical and monitoring equipment needed to care for critically ill patients.

The Australian and New Zealand Intensive Care Society (ANZICS) conducted a survey of Australian intensive care units (ICUs) in March 2020 to assess their readiness to respond to the COVID-19 pandemic. The findings discovered that there were 2183 staffed ICU beds available in 194 Australian ICUs (including five rural high dependency units), 884 of which were in New South Wales (40 percent). In that instance, there were 195 fewer intensive care units (8.2 percent) available in 2020 than there were in 2015. Overall number of ICU beds had decreased in all jurisdictions, but most significantly in rural/regional ICUs (59 fewer beds, an 18% loss) and private ICUs (140 fewer beds, 18 percent decline).[223]

Each day, around three to five patients are transported from regional ICUs to metropolitan or tertiary ICUs. Rural and regional ICUs are particularly vulnerable to demand exceeding capacity if the number of serious COVID-19 cases increased, for a variety of reasons, including the strain on inter-hospital transport systems and the fact that cancelling elective surgery provides less relief than cancelling elective surgery in metropolitan areas, where the elective ICU caseload is already generally lower. The disparities in ICU bed numbers per population between states may expose those with weaker capacity to additional strain if public health constraints lessen.[224]

[223] Litton, E, Huckson, S et.al, 2021

[224] Ibid

The chart below displays the number of public and private ICUs in Australia in 2020 and 2021.

		2020	2021			
ICU location/classification	Number of ICUs	Available, staffed ICU beds (per 100 000 population)	Available, staffed ICU beds (per 100 000 population)	Additional physical bed spaces in ICU	Additional bed spaces outside ICU	Total beds (per 100 000 population)
Australia	194	2378 (9.3)	2183 (8.5)	813	2627	5623 (21.9)
State/territory						
Australian Capital Territory	5	52 (12.1)	37 (8.6)	24	49	110 (25.5)
New South Wales	67	929 (11.4)	884 (10.8)	256	869	2009 (24.6)
Northern Territory	2	24 (9.7)	20 (8.1)	5	12	37 (15.0)
Queensland	42	418 (8.0)	408 (7.9)	178	490	1076 (20.7)
South Australia	12	201 (11.4)	161 (9.1)	61	127	349 (19.7)
Tasmania	5	59 (10.9)	38 (7.0)	26	38	102 (18.8)
Victoria	48	516 (7.7)	476 (7.1)	211	769	1456 (21.9)
Western Australia	13	179 (6.7)	159 (6.0)	52	273	484 (18.1)
Classification						
Tertiary	35	812	835	255	1009	2099
Paediatric	9	135	130	39	71	240
Metropolitan	34	316	302	177	346	825
Rural/regional	43	321	262	173	501	936
Private	73	794	654	169	700	1523

Demand for ICU services has not been consistent throughout the COVID-19 pandemic, and ICU resources are not uniformly dispersed throughout Australia. The COVID-19 pandemic has highlighted the tremendous impact it can have on Australia's hospital sector, with a lack of capacity to respond to surge demands which involve compromised staffing arrangements and care in new settings. The health care system is under pressure to provide adequate care for the general public and to redirect resources away from non-COVID-19-related medical illnesses and treatments.

The SOCI Act refers to assets within a critical infrastructure sector as ‘critical infrastructure assets’. Section 5 of the SOCI Act outlines the following in relation to a ‘critical hospital’:

*(5) An asset is a **critical hospital** if it is:*

(a) critical hospital means a hospital that has a general intensive care unit.

Note: The rules may prescribe that a specified critical hospital is not a critical infrastructure asset (see section 9).

Impacts of a disruption to critical hospital assets

- Disruption to procedures and surgeries putting patients and public safety at risk;
- Significant delays in getting treatments;
- Risk in increase mortality rates and serious conditions;;
- Shortages in or destruction of essential medical supplies; and
- Lack of accessible ICU capacity and hospital beds to meet high demands

Examples of disruptions to critical hospital assets – domestic and international

Gippsland and south-west Victoria (Barwon Health) Cyber Attack	Cyber security

Situation: On 30 September 2019, regional hospitals in Victoria, including Geelong and Latrobe, were hit by a ransomware cyber-attack. The attack brought the state's health care providers' computer systems to a stop. The cyber-attack resulted in the infiltration of ransomware, which left various systems, including financial management, inaccessible. Additionally, it stopped patient records, bookings, and management systems, requiring hospitals to return to manual processes and rely on paper records for the time being.[225]

Outcome: The cost of the cyber-attack event surpassed $3 million, according to the Barwon Health Annual Report 2019-20. Additionally, the incident posed a risk to patients' health, as several elective surgical operations and outpatient visits were cancelled as a result of the attack. Around two months after the ransomware attack, Barwon Health's systems were recovered, and staff email access was restored more than a month later.[226]

Identified Gap: The Victorian Audit General Office (VAGO) audited the health services following the cyberattack and determined that significant barriers to implementing cybersecurity controls developed by the Department of Health and Human Services (DHHS) included a lack of dedicated cybersecurity funding and limited staff availability and capability. Additionally, it was stated that hospitals lack the necessary mechanism in place to deal with a cyber incident.[227]

WannaCry Cyber-attack on National Health Service (NHS)	Cyber security

Situation: On 12 May 2017, a cyber-attack severely disrupted over 80 hospital trusts and 8% of GP practices in the NHS, after hospitals were locked down from a ransomware cyber-attack. Hospitals and GP surgeries across England and Scotland were forced to postpone appointments. The attack also resulted in the cancellation of 19,000 appointments over the one-week attack period, accounting for approximately 1% of all NHS care. The ransomware worked by preventing users from accessing 200,000 computers via red-lettered error messages demanding Bitcoin.[228]

Outcome: Although the attack disrupted approximately 1% of NHS care, the Department of Health and Social Care (DHSC) report stated that the attack cost approximately £20 million ($36 million AUD) in lost output, followed by another £72 million (130 million AUD) in IT support to restore data and systems. The total cost to the NHS was £92 million (equivalent to more than $168 million AUD) due to services lost during the attack and IT costs in the aftermath.[229]

Identified Gap: The attack's audit report revealed that there was no backup system in place and that the NHS had neglected to invest in technology. The Microsoft's Windows operating system is over 15 years old which is no longer up to date or supported. Microsoft only had the authority to fix the operating system. The UK's Government Communication Headquarters have been directed to develop a robust strategy to address future security issues and protect national IT infrastructure.[230]

Cyber-attack on Dusseldorf University Hospital	Cyber security

Situation: On 10 September 2020, a cyberattack taken down crucial systems at a University Hospital in Dusseldorf, western Germany. For a week, the University Clinic's systems were down, 30 of its clinic

[225] McDonald, 2018
[226] Ibid
[227] Ibid
[228] NHE, 2018
[229] Ibid
[230] Collier, 2017

computers were hacked, hospitals were unable to access data, emergency patients were transferred to other hospitals, and operations were postponed.[231]

Outcome: As a result of the ransomware attack, a woman who needed urgent admission and was in a life-threatening condition, died after she had to be taken to another city for treatment which was 32 kilometres away as doctors were unable to treat her. It has been reported that this could be the first recorded death from a ransomware attack.[232]

Identified Gap: According to reports, the hospital's information technology networks were compromised due to a weakness in Citrix, a vendor of a VPN tool. According to analysts from a cybersecurity firm, the hospital could have improved its security by implementing a Citrix software update that has been available for IT administrators to fix systems since January. They were also warned of the vulnerability back in January. As a result, audits and cyber security skill development in the workforce are critical components of protecting the infrastructure and resuming services with care and minimal interruption.[233]

Eastern Health Services (VIC) Cyber Attack	Cyber security, physical

Situation: On March 16, Eastern Health Services which operates in Box Hill, Maroondah, Healesville and Angliss Hospitals was forced to shut down some of its IT Systems following a widespread cyber-attack that crippled the server. Elective procedures were postponed, and staff were still unable to access internal emails and IT systems nearly two weeks after the attack, and they had reverted to utilising pen and paper and whiteboards for some patient management.[234]

Outcome: Due to doctors' difficulty in accessing hospital systems to gather patients' medical history, a frequent visitor to the hospital sought medical attention at Box Hill Hospital during the attack. The hospital staff treating him were unable to access his medical history, and due to his complicated needs, he was unable to express verbally to the doctor and nurses treating him that he had a history of diabetes and was in excruciating pain due to a swollen toe. He was discharged from the hospital with elevated blood sugar due to his diabetes, but they were unaware that he also had an infected toe. After visiting a podiatrist to have his sore toe examined, he was informed that the infection had gone to the bone.[235]

Identified Gap: The Australian Cyber Security Centre issued a critical alert for organisations that use Microsoft Exchange, stating that it has discovered major new vulnerabilities in the system which is used by eastern health services. The outdated IT infrastructure of Microsoft Exchange 2013, 2016, and 2019 enables attackers to get and keep access, highlighting how hospitals continue to rely on an outdated IT infrastructure that requires a substantial update to avoid serious disruptions in the future.[236]

Key risks to critical hospital assets

Hazard domain	Identified risk	Example
Physical and Natural	Increased occurrence of extreme weather events and natural disasters, including heatwaves, bushfires and floods, means critical hospital infrastructure is experiencing risks to protect the physical infrastructure and handle the surge in patients and account for enough beds.	On March 11, 2011, Fukushima was struck by a 9.0 magnitude earthquake and tsunamis that rose up to 41 metres. 11 hospitals in the disaster area experienced damage and critical building damage, 84 hospitals stopped accepting new inpatients and 45 hospital closed outpatient wards. The unprepared

[231] AP News, 2020
[232] Ibid
[233] Fortress, 2020
[234] Cunningham, 2021
[235] Ibid
[236] Ibid

		evacuation of hospitals caused increased mortality of patients, especially among the elderly. In the aftermath, there was much fear among hospital staff members about radiation exposure and many staff members failed to report to work.
Cyber	Healthcare is one of the industries hit particularly hard by cyber criminals. Cyberattacks on health care systems have spiked during the COVID-19 pandemic, threatening patient care and private data. Hospitals are then forced to turn off all online systems, which results staff being unable to provide services at full capacity and delayed procedures.	Between June-July 2018, Singapore's health system, 'SingHealth' was a target of a major cyber-attack. The attack caused a security breach that compromised 1.5 million SingHealth patients including Prime Minister Lee Hsien Loong. The incident also compromised outpatient medical data of 160,000 patients that visited the healthcare provider's facilities, which included four public hospital, nine polyclinics and 42 clinical specialities. The cost of the cyber-attack cost Singapore's public health sector around 250,000 AUD and around 770,000 AUD on financial penalties for the data breaches.
Supply Chain	Disruption to supply chains pertinent to critical hospitals may have detrimental consequences, as many procedures and services required for patient care and treatments are sourced domestically and internationally. This risk is compounded where organisations are primarily reliant on suppliers concentrated in a particular part of the world and may be concurrently affected by supply chain disruptions.	The COVID-19 pandemic incited concern that the health manufacturing and delivery of materials required for the maintenance of key pieces of hospital providers maybe delayed. The delay of deliveries of medical supply chains has strained hospitals in Australia and further states to undergo patient treatments and procedures.
Personnel	Where personnel are immobilised for reasons that cannot be controlled, critical hospital operations may be severely delayed or halted. Staff at facilities will not have the full ability to care or existing and incoming patients, potentially creating a surge. Additionally, personnel with access to systems, data or premises may pose insider threat risks including fraud, theft, espionage, infrastructure sabotage and misuse of sensitive data	The COVID-19 pandemic saw key industry personnel subject to extended periods of quarantine, forcing the shortage of staff, remote technology with limited protection or reduced capacity where insufficient personnel were available.

Existing legislation related to critical hospital assets

Overview of regulation		Identified gaps
National Health Security Act 2007 (Cth)	Establishes a framework for clear, quick and informed decision making to support a coordinated national response to public health emergencies. It also supports the exchange of information about significant public health events and authorises the disclosure of personal information when required to support an effective national or international response.	While the Act enables the exchange of public health information of national significance, there is lack of RMPs, mandatory cyber incident reporting, enhanced cyber security obligations for systems.
My Health Records Act 2012 (Cth)	The Act establishes the My Health Record system. The My Health Record system contains online summaries of individual's health information which can be viewed by their registered treating healthcare providers, including doctors, nurses and pharmacists	While the Act has safeguards implements around digital infrastructure, there is lack of RMPs, mandatory cyber incident reporting, enhanced cyber

Overview of regulation		Identified gaps
	across Australia. It limits when and how health information included in a My Health Record can be collected, used and disclosed. Unauthorised collection use or disclosure of My Health Record information is both a breach of the My Health Records Act and an interference with privacy. The equivalent State and Territory Acts include: • *Victorian Health Records Act 2001* • Health Records and Information Privacy Act 2002 (NSW) • Personal Information Protection Act 2004 (Tas) • *Hospital* and *Health* Boards *Act* 2011 (QLD) • Health Records (Privacy and Access) Act 1997 (ACT) • Information Act 2002 (NT)	security obligations for systems of national significance and the introduction of government assistance in responding to significant cyber-attacks.
Human Services (Medicare) Act 1973 (Cth)	The Act Creates the statutory office of the Chief Executive Medicare within the Department of Human Services and determines Chief Executive Medicare's functions including service delivery functions, functions conferred by other Acts and Medicare functions.	The Act lacks a framework for protecting data on Medicare services, posing a threat to numerous health records. Given the legislation's date of enactment, it is also out of time, as it excludes RMPmes for future cyber security incidents.
Privacy Act 1988 (Cth)	The Act protects the privacy of individuals and to regulate how Australian Government agencies and organisations with an annual turnover of more than $3 million, and some other organisations, handle information. The Privacy Act includes 13 Australian Privacy Principles (APPs), which apply to some private sector organisations, as well as most Australian Government agencies.	The State and territory public hospitals and health services are not covered by the Privacy Act, and only covered by relevant state or territory legislation. In addition, there aren't any risk management obligations and cyber security incident reporting imposed on a whole-of-sector basis.
The Health Insurance *Act 1973*	The Health Insurance *Act 1973* underpins the *Medicare* scheme by providing for payments by way of medical benefits and for hospital *services*.	There is lack of RMPs mandatory cyber incident reporting, enhanced cyber security obligations in supporting the hospital services in the Act. The systems of national significance and responding to significant cyber-attacks lacks the protection to the hospital services data and payments under the Medicare scheme.
Health Records Regulations 2012	A key objective of the regulations is to strike an appropriate balance between allowing adequate cost recovery for organisations and not setting maximum fees that are prohibitive for applicants. These regulations apply when an individual is exercising a statutory right to obtain access to, or requests the transfer of, health information under the Act.	While the regulation establishes protocols for obtaining access to health information, it lacks a risk management strategy for cyber security and data protection that would minimise stolen information and disruption.

Existing standards, guidelines and regulators for critical hospital assets

Hazard domain	Organisations	Description
Cyber	The Royal Australian College of Australian Practitioners (RACGP) Australian Digital Health Agency (ADHA) National Standards Institute of Technology (NIST)	Key industry and government stakeholders and leverage existing best practice standards for cyber security and safety, from Australia and overseas. • Information Security in General Practice • Information security guide for small healthcare businesses • NIST Cybersecurity Programs
	International Organization for Standardization (ISO)	**ISO 27001** provides requirements for information security management systems.

Jurisdiction	Regulator/s
Commonwealth	The Department of Health Therapeutic Goods Administration Private Health Insurance Ombudsman
Australian Capital Territory	ACT Health
New South Wales	NSW Health
Northern Territory	NT Health
Queensland	QLD Health
South Australia	SA Health
Tasmania	Tasmanian Department of Health
Victoria	Victoria Government Department of Health
Western Australia	Government of Western Australia Department of Health

Additional information on consultation

Overview of stakeholders consulted

Stakeholders Consulted

- Biogen
- CSL Limited
- Johnson & Johnson
- Roche Product Pty Ltd
- Ability Centre Australasia Limited
- National Blood Authority
- Therapeutic Goods Administration
- Health Direct
- Medicines Australia
- Epworth HealthCare
- Icon Group
- Monash Health
- Ramsay Health Care
- Rehab Management
- Sigma Healthcare
- St John of God Health Care
- Telstra Health
- UnitingCare
- Monash Health
- Royal Flying Doctor Service
- Australian & New Zealand Burn Association
- Australian Medical Association
- Australian Private Hospitals Association
- Australian Red Cross Blood Service
- Consumer Healthcare Products Australia
- Epworth HealthCare (Epworth Eastern (Box Hill))
- Epworth HealthCare (Epworth Freemasons (Melbourne))
- Epworth HealthCare (Epworth Hospital (Geelong))
- Epworth HealthCare (Epworth Richmond)
- Goulburn Valley Health (Goulburn Valley Health (Shepparton))
- Grampians Health (Ballarat Hospital)
- Healthecare (Mulgrave Private Hospital)
- Healthscope (Melbourne Private Hospital)
- Healthscope (Holmesglen Private Hospital)
- Healthscope (John Fawkner Private Hospital (Coburg))
- Healthscope (Knox Private Hospital)
- Latrobe Regional Hospital (Latrobe Regional Hospital)
- Melbourne Health (Royal Melbourne Hospital)
- Mercy Health (Werribee)
- Mercy Hospital
- Monash Health (Casey Hospital, Dandenong Hospital, Monash Children's Hospital, Monash Medical Centre)
- Monash Health (Jessie McPherson Private Hospital)
- Northern Health (Northern Hospital)
- Peninsula Health (Frankston Hospital)

Stakeholders Consulted	
• Council of Ambulance Authorities • Medical Technology Association of Australia • Medicines Australia • National Pharmaceutical Services Association • Merck Sharp & Dohme • Healthscope • Ambulance Victoria • Cochlear • Australian Nursing and Midwifery Federation • ACHA Health • St Andrews Hospital • Calvary Healthcare • Western Hospital • Department for Health and Wellbeing • Women's and Children's Health Network • Southern Adelaide Local Health Network • Central Adelaide Local Health Network • Northern Adelaide Local Health Network • Ramsay Health Care • UnitingCare Queensland • Albury Wodonga Health (Albury Hospital) • Alfred Health (The Alfred (Prahran)) • Austin Health (Austin Hospital (Heidelberg)) • Barwon Health (University Hospital (Geelong)) • Bendigo Health (Bendigo Health Hospital) • Cabrini Health (Cabrini Hospital (Malvern)) • Eastern Health (Angliss Hospital, Box Hill • Hospital, Maroondah Hospital) • Eastern Health (Angliss Hospital, Box Hill Hospital, Maroondah Hospital)	• Ramsay Health (Peninsula Private Hospital) • Ramsay Health (Warringal Private Hospital (Heidelberg)) • Royal Children's Hospital (Royal Children's Hospital) • Royal Women's Hospital (Royal Women's Hospital) • St John of God Healthcare (St John of God Ballarat Hospital) • St John of God Healthcare (St John of God Bendigo Hospital) • St John of God Healthcare (St John of God Berwick Hospital) • St John of God Healthcare (St John of God Geelong Hospital) • St Vincent's Health (St Vincent's Private Hospital Fitzroy) • St Vincent's Health Australia (St Vincent's Hospital Fitzroy) • The Bays Healthcare Group (The Bays Hospital) • Western Health (Footscray Hospital, Sunshine Hospital) • Representatives from Public and Private Hospital ICUs nationally.

RMP Rules consultation

The Department undertook extensive consultation with industry, including the hospital sector for the design of RMP rules, with the objectives of:

- Assessing whether there are existing regulations that meet the Bill's RMP objectives, to ensure the regulatory burden is reduced where possible; and
- Ensuring there are rules in place that will drive an uplift in the security and resilience of critical hospitals.[237]

Consultation with industry stakeholders occurred across the following key stages:

1. **A virtual Town Hall**, held on 19 October 2021, attended by 360 approximately industry and Government stakeholders, including from the critical hospitals sector. The purposes of the session were to:
   i. Outline the CI/SONS reforms and provide an update on the SLACI Bill (now SLACI Act) and SLACIP Bill (now SLACIP Act);
   ii. Provide an update for industry on the decision to consult on sector-agnostic RMP rules (as opposed to sector-specific rules), and outline how this would affect the consultation process going forward; and
   iii. Answer any questions about the Bills or RMP rules consultation process.
2. **Two critical hospitals-specific Information Sessions,** held on 12 and 24 November 2021, attended by approximately 180 and 75 industry and Government stakeholders respectively. The purpose of the information sessions was to reiterate the update for industry on the move from sector-specific to sector-agnostic RMP rules and to gain sector-specific feedback on the RMP rules.
3. **A final virtual Town Hall** held on 25 November 2021. The purpose of the Town Hall was to present the updated RMP rules and provide information on the further consultation period. The Town Hall was attended by approximately 800 industry and Government stakeholders across the 10 critical infrastructure sectors, including by stakeholders from the critical hospitals sector.
4. **Out of session consultation**:
   – Stakeholders were encouraged to contact the Department out of session. The Department availed itself to stakeholders to discuss their concerns, working to ensure stakeholders' understanding of the rules, and the rules' proportionality.
   – Out of session engagement also assisted in the iterative development of rules between workshops, through addressing concerns raised by individual stakeholders and proposing a solution.
   – This engagement strengthened the relationship between the Department and industry, while providing insights on implementation costs, entities' operating environments and the overall impacts of the proposed regulatory changes.
5. **Mandatory Public Consultation**, following the Minister commencing a 45-day consultation period on 5 October 2022 (the mandatory period is 28 days). Consultation included two Town Hall Sessions held on 10 October and 12 October 2022, attended by approximately 550 industry and Government stakeholders (across both sessions). The sessions provided information on the proposed RMP Rules as well as the broader obligation. These Town Halls,

[237] Department of Home Affairs 2021, 2

as well as four subsequent question and answer sessions, provided an opportunity for industry to ask questions about the proposed RMP Rules and process.

Outcomes and themes from consultation on RMP rules

Key themes from consultation

Rule category	Identified themes		Impact on development of rules
RMP rules	**Information sessions**	• The sector **acknowledges the emerging and increasing threats** to its critical infrastructure across all hazards. • The sector expressed a desire to **avoid regulatory duplication.** • The sector expressed some concerns regarding **timelines** for implementation. • Some expressed a desire to **broaden the asset definition** to adequate secure the sector, however some were content with the definition. • There is an **appetite for guidance material** to support sector-specific uplift in security and resilience, particularly for cybersecurity and supply chain hazards, potentially involving scenario-based examples.	In response to feedback received during the information sessions, the Department committed to: • Allowing responsible entities to leverage existing reporting requirements where appropriate, reflecting this in the rules and guidance material; • Taking a collaborative and educational approach to regulatory compliance, involving ongoing discussions around implementation (discussed further in section 7.1.3); and • Having ongoing discussions with industry to confirm the appropriateness of the asset definition; and • The development of guidance materials, which would highlight aspects of risk management that should be prioritised by responsible entities, assist industry in interpreting and implementing the rules to achieve an uplift in security and resilience, and address any concerns.

Consultation on costs

During the second information session, attendees were invited to participate in cost impact data collection through the completion of a cost impact template. This template was designed to collect substantive costing data to supplement the anecdotal costing discussions which had occurred throughout the workshop series. Industry were asked to provide:

- Their demographic information;
- Effort and cost estimates split by one-off and ongoing costs, staff effort, capital and other operating costs, and an estimated range between expected costs and highest possible costs; and
- Any comments on key boundaries, assumptions and cost drivers attached to the costing estimates provided.

Industry was provided with the template on 24 November 2021, with submissions open for a period of four weeks and closing on 22 December 2021.

The absence of entities within the sector that meet the definition of a small business indicated that consultation with the Australian Small Business and Family Enterprise Ombudsman was not required to identify expected costs to small businesses in preparing this RIS.[238]

[238] Office of Best Regulation Practice, 2021

Appendix P: Supplementary information for critical energy market operator assets

Overview of the role of energy market operators in Australia

Electricity and gas are major contributors to Australia's economy and essential to efficiently conduct almost all day-to-day activities. Energy market operators manage electricity and gas systems and markets across Australia.

The Australian Energy Market Operator (AEMO) manages most wholesale and retail electricity and gas markets nationally, including the National Energy Market (NEM), servicing over 22 million Australians across the six eastern and southern states and territories, and the (WEM) in Western Australia. Meanwhile, PowerWater operates the Northern Territory Electricity Market (I-NTEM), Horizon Power operates electricity markets in regional Western Australia and Western Power operates the South Western Interconnected System (SWIS) in south-western WA.

Their main activities are as follows:

- **Maintaining the security and reliability** of energy markets, which includes monitoring system performance and conducting forecasting to ensure supply meets demand, and crucially, restoring energy systems in the event of a disruption, which may involve coordinating with emergency management and state and territory governments.
- **Operating the whole and retail energy markets** for the buying and selling of energy, which includes registering market participants, overseeing wholesale trading, managing electricity dispatch, operating retail market infrastructure and providing timely market data.[239]

The SOCI Act refers to assets within a critical infrastructure sector as 'critical infrastructure assets'. Section 10 of the SOCI Act outlines the following in relation to 'critical energy market operator assets':

Critical energy market operator asset *means an asset that:*

(a) is owned or operated by:

(i) Australian Energy Market Operator Limited (ACN 32 072 010 327); or

(ii) Power and Water Corporation; or

(iii) Regional Power Corporation; or

(iv) Electricity Networks Corporation; and

(b) is used in connection with the operation of an energy market or system; and

(c) is critical to ensuring the security and reliability of an energy market; but does not include:

(d) a critical electricity asset; or

(e) a critical gas asset; or

(f) a critical liquid fuel asset.

[239] AEMO, 2021

Impacts of a disruption to critical energy market operator assets

The consequences of a prolonged and widespread disruption to a critical energy market operator asset may include:

- Disruption to electricity, gas and water assets;
- Delays to the restoration of disrupted electricity, gas and water assets;
- Disruption to telecommunications networks which are dependent on electricity;
- Disruptions to transport infrastructure, traffic management systems and fuel supplies;
- Reduced services or closure of banking, finance and retail sectors dependent on electricity;
- An inability for businesses and governments to function as normal; and
- A reduction in business and market confidence.

Examples of disruptions to critical energy market operator assets – domestic and international

Australia's summer bushfires threaten electricity grid (2020)	**Natural hazard & physical risk**
Situation: The Australian bushfires in the summer of 2020, which destroyed more than 10 million hectares of land and killed more than a billion animals, saw unprecedented pressure on Australia's electricity grid. While the biggest potential threat, that bushfires would strike the critical interconnector linking the Victorian and New South Wales electricity grids, was not realised, accompanying extreme hot weather saw significant increases in the demand for electricity.[240]	
Outcome: The combination of catastrophic bushfires and extreme weather conditions saw some Australian customers without electricity for an extended period. The Australian Energy Market Operator (AEMO) issued a level two 'lack of reserve' warning and signalled a potential need to call on emergency power reserves to avoid widespread blackouts. Approximately 10,000 customers in the Tumbarumba and South Coast regions, as well as an additional 5,800 were without electricity between New Years Eve of 2019 and early January 2020.[241]	
Identified Gap: Rural towns and those residing on the edge of the electricity grid had no or insufficient back-up supplies or lacked a contingency plan. This caused power outages across regional communities and meant some critical energy assets were unable to sustain operation for the duration of the bushfire disaster. The continued emergency reflected the need for regional market operators to have thorough RMPs which reflect ways to mitigate the risks associated with the increase in natural hazards such as bushfires to prevent outages in the provision of electricity during times of emergency.	

Ukraine's extended power disruptions (2015)	**Physical**
Situation: On 23 December 2015, malicious actors launched a sophisticated attack on the Ukrainian power grid, taking control of three energy distributors' Supervisory Control and Data Acquisition Networks. The attack saw the malicious actors attain remote access to and control over the firms' computers, allowing	

[240] Foley, 2020

[241] Ibid

circuit breakers to be tripped and eventually taking thirty substations offline. Attackers also sought to disable or destroy other digital infrastructure, by wiping essential data from the companies' networks. Concurrently, a call centre that provided up to date information to consumers about the blackout was rendered inoperable due to a denial-of-service attack.

Outcome: While less than 1 per cent of the country's daily consumption of energy was disrupted, the attack left over 225,000 Ukrainians, in the middle of winter, without power for several hours. Two months after the attack, some substations were still not fully operational and required manual operation to continue functioning.

Identified Gap: The attack is believed to be the first known cyber intrusion with success in downing the operation of a power grid. This incident highlights that while it is imperative to ensure the protection of critical energy market operator assets, supplementary and connected services must also be protected. For example, the disruption of the Ukraine power plant's customer service centre heightened, and prolonged, the effects of the attack itself.

Malware attack on Saudi Arabian petrochemical plant (2017)	Physical, cyber & personnel risk

Situation: In 2017, hackers deployed malware on a Saudi Arabian petrochemical plant, which allowed remote access to and control over the plant's safety systems. The safety systems were designed as a 'last line of defence' against plant malfunctions, supporting plant processes in returning to safe levels or forcing them to cease operating where the threat of continued operation was too great.[1] The malware deployed to conduct the intrusion is widely suspected to be built by a nation-state actor.[242]

Outcome: A flaw in the hackers' code meant their infiltration operation was ultimately unsuccessful. However, had the hackers' infiltration been successful, it could have led to the release of toxic hydrogen sulphide gas or prompted explosions, putting at risk the lives of those who work at the facility and those in the surrounding area.[1]

Identified Gap: The attack highlighted the need for entities to maintain pace with evolving malware capabilities and work to strengthen their 'last line of defence'. Without adequate protections and consistent re-evaluations, operating systems considered critical to defending against catastrophic events, may be compromised.[243]

Japan's earthquake and tsunami cause blackouts (2011)	Physical

Situation: In March 2011, Japan experienced its strongest earthquake in history, which subsequently caused the Tohoku tsunami – producing waves of up to 40 meters. Following the disaster, large parts of Japan were plunged into darkness amid rolling blackouts caused from a drastic reduction in the supply of electricity. At the time of the incident, Japan relied on nuclear energy for approximately one quarter of its electricity. Of the country's 54 reactors, 11 were forced to close following the disaster, leaving 2.6 million households without power.[244]

Outcome: Environmental risks, such as natural disasters and weather events, are categorised as an

[242] Gonzalez, 2021
[243] Ibid
[244] Branigan, 2011

external supply chain risk, with the Australian Productivity Commission recognising Japan's 2011 disaster as an example of an environmental hazard which caused significant disruption of supply chains.[245] Following the earthquake and tsunami:

- Electricity rationing was introduced, to account for the country's power shortfall;
- Utility companies were forced to approach their top commercial and industrial customers to request that they cut back on their energy usage;
- Train operations were decreased by 30-50% in order to save power; and

In the longer term, Japan began importing additional oil, fuel and natural gas resources, to account for the shortfall in electricity generation.[246]

Identified Gap: The Australian Productivity Commission suggests that the consequences of disruption, such as those caused in Japan, can be mitigated through increased preparedness. Japan's 2011 disaster was compounded by the nation's geographic clustering of key electricity-related infrastructure. Such clustering caused extensive market-level vulnerabilities, as many firms in the electricity industry were affected.[247] Diversified supply chains and advanced contingency planning can assist in reducing the levels of disruption caused by environmental risks.[248]

Key risks to critical energy market operator assets

Risk	Identified risk	Example
Physical	Increased occurrence of extreme weather events and natural disasters, including heatwaves, bushfires and floods, means physical electricity infrastructure is experiencing heightened pressure. This stems from both increased demand for energy and the threat or realisation of damage to critical infrastructure, such as power plants, power lines and pipelines.	In 2016, a series of severe thunderstorms triggered a state-wide blackout in South Australia. The incident damaged transmission and distribution assets and resulted in the suspension of the state's wholesale market for thirteen hours.
	There is also a risk of sabotage by malicious actors to critical infrastructure's physical facilities. This could be used to disrupt the functioning of critical infrastructure and the systems which rely upon its function during times of heightened tension or conflict in the case of state-based actors.	In 1996 the Irish Republican Army (IRA) planned to disrupt the supply of electricity to the south east of England by destroying six electrical sub-stations with explosive devices. If the attack had been successful, there would have been a disruption in supply to the area for several months, with cascading disruptions across services reliant upon the electrical supply to function.[249]
Cyber	Market operators are becoming more reliant on software technology, to create more accurate market forecasts and data, as well as better collaborate across the grid and with emergency management. This creates the potential for unintended taint (where software design or implementation flaws increase susceptibility to cyber risks) and malicious taint (deliberate diversion or disruption to cyber	The AEMO has advised it is aware of sustained cyber-attack campaigns targeting Australia's electricity grid.[251] The AEMO advised that malicious actors such as the Avaddon Ransomware group had targeted more than 120 organisations globally, including critical infrastructure assets, with one Australian entity being attacked in early 2021.[252]

[245] Australian Government Productivity Commission, 2021
[246] Murphy, 2011
[247] Australian Government Productivity Commission, 2021
[248] Ibid
[249] Bennetto, 1997

Risk	Identified risk	Example
	supply chains intentionally introduces cyber risks).[250]	
Supply Chain	Disruption to supply chains pertinent to critical energy market operator assets may have detrimental consequences, as many project components and materials required for the maintenance of key pieces of energy infrastructure are sourced from international suppliers.[253] This risk is compounded where organisations are primarily reliant on suppliers concentrated in a particular part of the world and may be concurrently affected by supply chain disruptions.[254]	The COVID-19 pandemic incited concern that the manufacturing and delivery of materials required for the maintenance of key pieces of energy infrastructure be delayed, as required components must be sourced from Asia. Supply chain risks arose through the need for some electricity companies to cut back on capital and operational expenditures, which filtered down to suppliers and services companies who are reliant on upstream resources.[255]
Personnel	Where personnel are immobilised for reasons that cannot be controlled, critical energy market operator operations may be severely delayed or halted. Additionally, personnel with access to systems, data or premises may pose insider threat risks including fraud, theft, espionage, infrastructure sabotage and misuse of sensitive data.[256]	The COVID-19 pandemic saw key industry personnel subject to extended periods of quarantine, forcing the closure of some electricity generators or reduced capacity where insufficient personnel were available. Between 2013 and 2015, a series of attacks occurred on a company responsible for operating over 50 power plants across the US and Canada. The attacks were facilitated by information stolen by a company contractor and resulted in the theft of critical power plant designs and system passwords.[257]

Existing legislation related to critical energy market operator assets

Overview of regulation		Identified gaps
Electricity Industry Act 2004 (WA)	Establishes WA's Wholesale Energy market.	The Electricity Industry (Wholesale Electricity Market) Regulations 2004 outline that the market operator must ensure that 'SWIS is operated in a secure and reliable manner'. However, no risk management principles are specified.
National Electricity (South Australia) Act	Adopted as the model law, referred to as the National Electricity Law, and implemented (with minor amendments) across Australian State and Territory participants in the NEM.	The National Electricity Law is contained in a Schedule to the *National Electricity (South Australia) Act 1996* and seeks to establish the governance framework and

[251] Australian Energy Market Operator, 2019; Australian Energy Market Operator, 2018
[252] Australian Energy Market Operator, 2021
[250] Atlantic Council, 2018
[253] Chenneveau, 2020
[254] Kilpatrick, 2021
[255] Deloitte, 2020
[256] Ernst & Young, 2016
[257] Johnston, 2017

Overview of regulation		Identified gaps
1996	The equivalent State and Territory Acts include: • *Electricity (National Scheme) Act 1997* (ACT); • *National Electricity (New South Wales) Act 1997 No 20 & National Electricity (New South Wales) Law No 20a;* • *National Electricity (Northern Territory) (National Uniform Legislation) Act 2015;* • *Electricity – National Scheme (Queensland) Act 1997 & National Electricity (Queensland) Law;* • *Electricity – National Scheme (Tasmania) Act 1999 & National Electricity (Tasmania) Law; and* • *National Electricity (Victoria) Act 2005.* In Western Australia, the *Electricity Act 1945* and *Electricity Regulations 1947* operate, in addition to a series of other legislative frameworks. These schemes are similar in content and form to the National Electricity Law but operate as a separate regime.	key obligations for the NEM, including: • The functions of the AEMO; and • The regulation of access to electricity networks. The National Electricity Law is supported by the National Electricity Regulations and National Electricity Rules, which support the operation of the NEM. The National Electricity Law (and its subordinate legislation) does impose certain requirements on specific entities, with some implication for risk management. It requires the AEMO to maintain supply-demand balance (electrical supply security), but does not impose obligations around cyber, physical or other security. Furthermore, the National Electricity Law is primarily focussed on matters of governance and does not impose baseline risk reduction requirements on all entities. Finally, the National Electricity Law places obligations on AEMO to operate the system in a particular way, but it does not obligate AEMO to have an all hazards RMP.
Australian Energy Market Act 2004 (Cth)	Applies the National Electricity Law, the National Electricity Regulations and the National Electricity Rules as Commonwealth law in offshore areas as part of a uniform scheme of national electricity regulation. Also applies the National Gas Law, the National Gas Regulations and the National Gas Rules as Commonwealth law in offshore areas.	This Act has, largely, an administrative function in applying the National Electricity and Gas Law in offshore areas. It does include provisions supplementary to the National Electricity and Gas Law and therefore, does not impose risk reduction requirements.

National Gas (South Australia) Act 2008	Adopted as the model law, referred to as the National Gas Law, and implemented (with minor amendments) across Australian State and Territory participants in the National Gas Market. The equivalent State and Territory Acts include: • *National Gas (ACT) Act 2008;* • *National Gas (New South Wales) Act 2008 No 31 & National Gas (New South Wales) Law No 31a;* • *National Gas (Northern Territory) Act 2008;* • *National Gas (Queensland) Act 2008;* • *National Gas (Tasmania) Act 2008; and* • *National Gas (Victoria) Act 2008.* Western Australia participates in the National Gas Market to the extent set out in the *National Gas Access (WA) Act 2009*.	The National Gas Law is contained in a Schedule to the *National Gas (South Australia) Act 2008* and sets out a State and Territory access regime for gas pipelines, which are subject to either 'light' or 'full' regulation, if classified as 'covered' pipelines. A person seeking access to a natural gas pipeline must satisfy certain criteria before obtaining a statutory right of access.[258] The National Gas Law is supported by the National Gas Regulations and National Gas Rules, which govern access to natural gas pipeline services. However, the National Gas Law is focussed on access and licensing regimes. It does not impose baseline risk reduction requirements on entities.
State and Territory Emergency Management Legislation	Australia's States and Territories have in place emergency management legislation which may have a risk management element, including: • *Electricity Supply Act 1995 (NSW)* • *Essential Goods and Services Act 1981 (NT)* • *Electricity Reform Act 2000 (NT)* • *Fuel Energy and Resources Act 1972 (WA)* • *Essential Services Act 1981 (SA)* • *Electricity Industry Act 2000 (VIC)* • *Electricity Supply Industry Act 1995 (TAS)* • *Utilities Act 2000 (ACT)* • *Electricity Act 1994 (QLD)*	While the risk management element contained in these legislative regimes may contribute to suitable risk management, they do not amount to an all hazards approach to risk management, nor are risk management obligations imposed on a whole-of-sector basis.
Wholesale Electricity market (WEM) Rules WA	Guide the operation of the WEM, including the trading and dispatch of energy, the Reserve Capacity Mechanism and settlement. They also mandate governance of the WEM.	The Rules stipulate that the market operator must have an Operating Protocol with 'general principles and processes for security management and coordination' and for 'management of emergencies', as well as a process to determining and classifying 'credible contingency' events. However, it does not provide baseline standards of security management that must be met by the market operator(s).

[258] Cunsolo, n.d.

Existing standards, guidelines and regulators for critical energy market operator assets

Hazard domain	Organisation	Standards & guidelines
Cyber	AEMO Australian Cyber Security Centre (ACSC) Cyber and Infrastructure Security Centre Cyber Security Industry Working Group	**Australian Energy Sector Cyber Security Framework** (AESCSF) was developed with key industry and government stakeholders and leverages existing best practice standards for cyber security and safety, from Australia and overseas. The AESCSF incorporates the following Australian references: • ACSC Essential 8 Strategies to Mitigate Cyber Security Incidents; • The Australian Privacy Principles; and • The Notifiable Data Breaches Scheme.
	National Institutes of Standards and Technology (NIST)	**Cybersecurity Programs**
	International Organization for Standardization (ISO)	**ISO 27001** provides requirements for information security management systems.
	United States Department of Energy	**Cybersecurity Capability Maturity Model (C2M2)** was developed by the U.S. Department of Energy in conjunction with energy sector subject matter experts. It provides a voluntary evaluation process which allows entities to determine the maturity of their cyber security capabilities. The AESCSF is based upon this model.
	ACSC	**Essential Eight Maturity Model** provides requirements to increase business resilience against cyber and information security hazards.
	AEMO	**Power System Data Communication Standard** sets out the standards with which Data Communication Providers (DCPs) must comply when transmitting data to and from AEMO.
Natural Hazards	AEMO	**Reliability Standards Implementation Guidelines** The Guidelines set out how the Australian Energy Market Operator (AEMO) implements the reliability standard, including regarding the treatment of extreme weather events.

Jurisdiction	Regulator/s
Commonwealth	Australian Energy Regulator (Responsible for regulating wholesale and retail energy markets and energy networks, under national energy legislation and rules. The AER sets network prices so that energy consumers pay no more than necessary for the safe and reliable delivery of electricity services, which includes setting the maximum amount of revenue which can be earned by electricity networks. The AER's regulatory functions relate, in particular, to energy markets in eastern and southern Australia.) Australian Energy Market Operator Energy Security Board (Provides whole of system oversight on energy security and reliability.)
Northern Territory	Utilities Commission of the Northern Territory
Western Australia	Economic Regulation Authority of Western Australia

Additional information on consultation

Overview of stakeholders consulted

Stakeholders Consulted	
• Western Power	• The Australian Energy Market Operator (AEMO)
• Horizon Power	• Power and Water Corporation

RMP Rules consultation

Consultation with industry stakeholders occurred across the following key stages:

1. **A virtual town hall**, held in April 2021 attended by approximately 170 industry and Government stakeholders, to communicate the purpose of the co-design process and obtain information to inform the design of future workshops.
2. **A series of three virtual workshops for both energy market operators and the electricity sector**, held over a six-week period beginning in April 2021 and each attended by approximately 190 industry and Government stakeholders, including market operators, which provided a forum to design RMP Rules and assisted in understanding the costs and benefits associated with implementing the risk management program framework. Workshops were designed to provide:
   i. Several opportunities for discussion and feedback to gather industry perspectives;
   ii. Polling, in-session surveys and facilitated discussions; and
   iii. 'Break out room' discussions, divided into generators, transmitters and distributors, to ensure comprehensive discussion occurred across all subsets of industry.
3. **Out of session consultation**, including meetings with a number of stakeholders and extensive email communication.
   – Stakeholders were encouraged to contact the Department out of session. The Department availed itself to stakeholders to discuss their concerns, working to ensure stakeholders' understanding of the rules, and the rules' proportionality.

- Out of session engagement also assisted in the iterative development of rules between workshops, through addressing concerns raised by individual stakeholders and proposing a solution.
- This engagement strengthened the relationship between the Department and industry, while providing insights on implementation costs, entities' operating environments and the overall impacts of the proposed regulatory changes.

4. **A follow up consultation session and two industry-agnostic town halls** held from October to December 2021. The purpose of the consultation session was to provide an update for industry on the move from sector-specific to sector-agnostic RMP Rules and to gain sector-specific feedback on the updated RMP Rules. The purpose of the industry town hall was to present the updated RMP Rules and provide information on the further consultation period. The consultation session was attended by approximately 32 industry and Government stakeholders. The two town halls were attended by approximately 800 industry and Government stakeholders across the 10 critical infrastructure sectors, including many stakeholders from energy market operators.

5. **Mandatory Public Consultation**, following the Minister commencing a 45-day consultation period on 5 October 2022 (the mandatory period is 28 days). Consultation included two Town Hall Sessions held on 10 October and 12 October 2022, attended by approximately 550 industry and Government stakeholders (across both sessions). The sessions provided information on the proposed RMP Rules as well as the broader obligation. These Town Halls, as well as four subsequent question and answer sessions, provided an opportunity for industry to ask questions about the proposed RMP Rules and process.

Outcomes from consultation on Risk Management Program rules

Summary of Feedback from consultation sessions with responsible entities for critical energy market operator assets

Rule category	Identified themes		Impact on development of rules
Sector-agnostic RMP Rules	**Consultation Sessions**	• Industry believes the RMP Rules are **clear and understandable.** • Industry believes the RMP Rules will **be able to be implemented.** • The RMP Rules provide a **baseline** for sector resilience and security. • There is an **appetite for guidance material** to support sector-specific uplift in security and resilience.	In response to feedback received during the consultation sessions, the Department committed to: • The development of guidance materials, which would highlight aspects of risk management that should be prioritised by responsible entities and assist industry in interpreting and implementing the rules to achieve an uplift in security and resilience.

Consultation on costs

During the final consultation session, attendees were invited to participate in cost impact data collection through the completion of a cost impact template. This template was designed to collect

substantive costing data to supplement the anecdotal costing discussions which had occurred throughout the workshop series. Industry were asked to provide:

- Their demographic information;
- Effort and cost estimates split by one-off and ongoing costs, staff effort, capital and other operating costs, and an estimated range between expected costs and highest possible costs; and
- Any comments on key boundaries, assumptions and cost drivers attached to the costing estimates provided.

Industry was provided with the template on 8 December 2021, with submissions open for a period of four weeks and closing on 12 January 2022.

The absence of entities within the sector that meet the definition of a small business indicated that consultation with the Australian Small Business and Family Enterprise Ombudsman was not required to identify expected costs to small businesses in preparing this RIS.[259]

[259] Office of Best Regulation Practice, 2021

Appendix Q: Supplementary information for critical freight infrastructure and critical freight services assets

Overview of the role of freight infrastructure and freight services in Australia

Freight infrastructure and freight services incorporate the freight networks and service providers that use road, rail, and maritime infrastructure to transport nationally produced goods and products for domestic consumption and to facilitate imports and exports. Freight infrastructure and services form crucial parts of the supply chain for Australian imports, exports, and domestic consumption.

Critical freight infrastructure refers to the critical corridors for the transportation of goods while critical freight service providers that conduct business that is essential to the transportation of goods. These include road, rail, maritime or intermodal transfer facilities, or entities that operate within these freight subsets.

The SOCI Act refers to assets within a critical infrastructure sector as 'critical infrastructure assets'. Section 12B and 12C of the SOCI Act provide the following in relation to 'critical freight infrastructure and services assets':

*An asset is a **critical freight infrastructure and services asset** if it is:*

(1) *An asset is a **critical freight infrastructure asset** if it is any of the following:*

(a) a road network that, in accordance with subsection (2), functions as a critical corridor for the transportation of goods between:

(i) 2 States; or

(ii) a State and a Territory; or

(iii) 2 Territories; or

(iv) 2 regional centres;

(b) a rail network that, in accordance with subsection (3), functions as a critical corridor for the transportation of goods between:

(i) 2 States; or

(ii) a State and a Territory; or

(iii) 2 Territories; or

(iv) 2 regional centres;

(c) an intermodal transfer facility that, in accordance with subsection (4), is critical to the transportation of goods between:

(i) 2 States; or

(ii) a State and a Territory; or

(iii) 2 Territories; or

(iv) 2 regional centres.

(2) specified road networks that function as a critical corridor for the transportation of goods between:

(i) 2 States; or

(ii) a State and a Territory; or

(iii) 2 Territories; or

(iv) 2 regional centres; or

(b) requirements for a road network to function as a critical corridor for the transportation of goods between:

(i) 2 States; or

(ii) a State and a Territory; or

(iii) 2 Territories; or

(iv) 2 regional centres.

(3) For the purposes of paragraph (1)(b), the rules may prescribe:

(a) specified rail networks that function as a critical corridor for the transportation of goods between:

(i) 2 States; or

(ii) a State and a Territory; or

(iii) 2 Territories; or

(iv) 2 regional centres; or

(b) requirements for a rail network to function as a critical corridor for the transportation of goods between:

(i) 2 States; or

(ii) a State and a Territory; or

(iii) 2 Territories; or

(iv) 2 regional centres.

(4) For the purposes of paragraph (1)(c), the rules may prescribe:

(a) specified intermodal transfer facilities that are critical to the transportation of goods between:

(i) 2 States; or

(ii) a State and a Territory; or

(iii) 2 Territories; or

(iv) 2 regional centres; or

(b) requirements for an intermodal transfer facility to be critical to the transportation of goods between:

(i) 2 States; or

(ii) a State and a Territory; or

(iv) 2 Territories; or

(v) 2 regional centres.

*(1) An asset is a **critical freight services asset** if it is a network that is used by an entity carrying on a business that, in accordance with subsection (2), is critical to the transportation of goods by any or all of the following:*

(a) road;

(b) rail;

(c) inland waters;

(d) sea.

(2) For the purposes of subsection (1), the rules may prescribe:

(a) specified businesses that are critical to the transportation of goods by any or all of the following:

(i) road;

(ii) rail;

(iii) inland waters;

(iv) sea; or

(b) requirements for a business to be critical to the transportation of goods by any or all of the following:

(i) road;

(ii) rail;

(iii) inland waters;

(iv) sea.

Impacts of a disruption to critical freight infrastructure and freight services assets

- Reduced access to supplies, such as food, medicine, building and agricultural supplies, due to reduced ability to transport domestically, import and export;
- Reduced access to critical infrastructure such as critical supermarkets, particularly for regional and remote Australians;
- Reduced fuel supply due to an inability to transport, with flow on effects to consumers and industry;
- Reduced economic activity and increased inflationary pressures; and
- Increased vulnerability to natural disasters, with reduced ability to deploy emergency services personnel in the event of a natural disaster.
- Examples of disruptions to critical freight assets – domestic and international

Maersk hit in NotPeyta attack, Global, 2017	**Cyber & Personnel Risk**
Situation: Maersk is a Danish shipping company, the largest in the world, that provides integrated container logistics and supply chain services globally, including to Australia. In 2017, Maersk was one of the victims of a sophisticated cyber attack spree that hit a list of companies. NotPeyta was the malware responsible for attacking communications, IT systems, critical systems and operational controls company wide. The malware was spread via the Microsoft Windows systems to almost all offices across 130 countries.[260,261]	
Outcome: The attack destroyed all end-user devices including laptops, print capability, applications, communications, and servers. Requiring almost a complete infrastructure overhaul, Maersk was forced to reinstall 45,000 PCs, 2,500 applications, and 4,000 servers to recover from the attack, costing $300 million USD. The company was forced to reduce operational volume to 80% during the recovery.[262]	

[260] Global Intelligence for Digital Leaders, 2019

[261] ZDNet, 2018

[262] Digital Guardian, 2020

Identified Gap: Maersk fell victim to the attack through a member of staff responding to an email infected with the NotPeyta malware. The incident demonstrates the importance of cyber security training of personnel and internal detection systems. Increased cyber security training and better detection systems may have dramatically reduced or removed the threat entirely.

TNT Express targeted in NotPeyta attack, Global, 2017	Cyber Risk

Situation: FedEx subsidiary company, TNT, also fell victim to the global wave of NotPeyta malware and ransomware attacks in 2017. The cyber-attack disrupted computer systems and IT operations which caused deliveries and sales to suffer in all countries of operation, including Australia. It is believed the company was exposed to the ransomware via an infected tax software update used by its Ukrainian office.[263]

Outcome: FedEx reported that the ransomware attack cost TNT approximately USD300.0 million (AUD416.7 million AUD) in lost earnings due to disruptions in the company's operations, loss of information technology systems and extended recovery times.[264,265]

Identified Gap: The incident highlighted the lack of cyber security protocols in their operations, finance, back-office and secondary business systems.

Forward Air Ransomware attack, North America, 2020	Cyber & Personnel Risk

Situation: Forward Air, an air freight shipping company operating in the United States and Canada, was the subject of a ransomware attack in December 2020. The incident impacted the operation and information technology systems and included a data breech. The company suspended all electronic customer databases temporarily to limit the impact of the attack.[266,267]

Outcome: The attack cost Forward Air $7.5 million USD (AUD 10.4 million) in less than load freight revenue as a result the required temporary suspension of the electronic data interfaces with its customers.[268]

Identified Gap: While it is unclear exactly how Forward Air fell victim to the Hades ransomware attack, the incident demonstrates the importance of having proactive risk management processes in place to identify and contain cyber risks and the risks posed by malicious insiders.

BHP runaway train, Port Hedland, Western Australia, 2018	Physical & Personnel Risk

Situation: BHP was forced to derail a runaway iron ore train that was fully laden, after the train had travelled for over 50 minutes without a driver. The forced stop destroyed over 1.5km of railway tracks. The 268-wagon train was carrying 30,000 tonnes of iron ore at the time of the incident, with all but 24 wagons damaged[269].

When exiting the train to carry out an inspection, the driver of the train failed to engage the emergency brake as required by the relevant operating procedures, which led to the backup braking system failing to operate and automatically releasing after an hour while the driver was still outside the train[270]. It should be

[263] BBC News, 2017
[264] ZDNet, 2017
[265] ZDNet, 2017
[266] Heimdal Security, 2021
[267] Silicon Angle, 2021
[268] Bleeping Computer, 2021
[269] Financial Review, 2019
[270] ABC News, 2019

noted that maintenance workers had mistakenly applied brakes to the wrong locomotive in the last year prior to the incident[271].

It is understood that the AutoHaul system being introduced by Rio Tinto may have been able to stop the runaway train, with the company moving to introduce driverless trains in the near future.[272]

Outcome: The disruption, including lost product, was anticipated to have cost the company up to $600 million with an estimated loss of $55 million in revenue per day, since BHP could not ship iron ore to its Asian customers[273]. As a result of the incident, there was a 4 million tonne production loss, with BHP iron ore productivity down by 6%[274].

Identified Gap: The incident highlighted the need for more intensive personnel and physical security protocol training. Maintenance workers and train drivers may require additional training to prevent reoccurrences. There is a clear gap in protocol with the central switch board receiving information pertaining to the incident and in their response. Physical infrastructure provides another opportunity to solidify critical infrastructure that may prevent future compromises.

Key risks to critical freight assets

Hazard domain	Identified risk	Example
Physical & Natural Hazard	An increase in extreme weather events across Australia and the world, including heatwaves, bushfires and flooding, can undermine the physical security of critical freight infrastructure assets and impair operations of critical freight services by placing such assets under strain. Drought and subsequent flooding events also have the ability to create significant flow on effects that may directly or indirectly affect other critical infrastructure assets.	Due to heavy rain and flooding occurring across Queensland in Spring 2021, after 180mm of rain fell in 24 hours, over 400 roads were closed. Dams and rivers threatened to burst their banks, affecting major roadways in regions across the states south-east, including Ipswich, Brisbane, Gold Coast, Logan, Scenic Rim, Moreton Bay, Sunshine Coast, Toowoomba and the Darling Downs.[275] The severe 2019 bushfire season also highlighted the vulnerability of critical freight assets to natural disaster, seeing over 100 major roads closed across Victoria, New South Wales and South Australia due to fire conditions.[276]
	There is also a risk of sabotage by malicious actors to critical infrastructure's physical facilities. This could be used to disrupt the functioning of critical infrastructure and the systems which rely upon its function during times of heightened tension or conflict in the case of state-based actors. Alternatively, critical freight infrastructure and services may be subject to disruption or damage to physical assets due to non-malicious personnel faults.	BHP was forced to derail a runaway iron ore train that was fully laden, after the train had travelled for over 50 minutes without a driver. The forced stop destroyed over 1.5km of railway tracks. The 268-wagon train was carrying 30,000 tonnes of iron ore at the time of the incident, with all but 24 wagons damaged. The train was initially stopped after a braking system control cable became disconnected, leading the driver of the train to exit the train to carry out an inspection. The driver of the train failed to engage the emergency brake as required by the relevant operating procedures, which led to the backup braking system failing

[271] The Guardian, 2019
[272] PerthNow, 2018
[273] ABC News, 2019 ; PerthNow, 2018
[274] Financial Review, 2019
[275] The Courier Mail, 2020
[276] Sutton and Brown, 2020

Hazard domain	Identified risk	Example
		to operate and was automatically released after an hour while the driver was still outside the train.[277,278]
Cyber	Information Technology (IT) and Operational Technology (OT) systems are becoming integrated more frequently. IT refers to software applications with capabilities in process management, resource allocation and decision-making, while OT allows for the operational control of assets within the network, in real time. The integration of OT and IT is desirable as the applications are able to work in tandem to optimise a holistic operational approach. However, as this convergence occurs, it provides more opportunity to malicious actors, including but not limited to exploiting backdoor vulnerabilities or increased risk of personnel exposing a system to malware, phishing, or other cyber attacks.	Global shipping companies Maerk and FedEx subsidiary TNT fell victim to NotPeyta malware and ransomware attacks that targeted hundreds of companies in 2017. The companies both experienced failures across their information and operational technology systems, with the attack resulting in fatal errors to a significant proportion of both companies' technology systems. There was a direct blow to operational volume and lost earnings by both companies.[279,280,281]
Supply Chain	Disruption to or overwhelming of supply chains pertinent to critical freight infrastructure and services assets may have detrimental consequences. This may include causing physical failure of freight infrastructure or overburdening freight services to the point of mass failure of systems and services.	Shipping and freight costs in Australia have increased because of the influx of demand on the global supply chain due to COVID-19, leading to the import and export exceeding capacity of ports across the country. Due to the restrictions on travel, trade has seen enormous pressure to cope with increasing demand on decreasing availability of freight options. Australia imports substantially more than they export, leading to a build-up of empty shipping containers that are both exacerbated the acute worldwide shortage of shipping containers. This has resulted in increased costs and a blowout in delays.[282,283,284,285]
Personnel	Where personnel are immobilised for reasons that cannot be controlled, critical freight operations may be severely delayed or halted. Additionally, personnel with access to systems, data or premises may pose insider threat risks including fraud, theft, espionage, infrastructure sabotage and misuse of sensitive data. Alternatively, personnel may be responsible for major	The COVID-19 pandemic saw personnel and critical freight services subject to extended periods of quarantine and shutdown, often leading to understaffing and significantly increased pressure and workload. Additionally, workers faced poor working conditions partially as a result of enduring two cyber-attacks on Toll companies combined with high volume intense periods over Christmas and frequent late

[277] Financial Review, 2019
[278] ABC News, 2019
[279] Global Intelligence for Digital Leaders, 2019
[280] ZDNet, 2018
[281] BBC News, 2017
[282] ABC News, 2021
[283] Financial Review, 2021
[284] ABC News, 2021
[285] Financial Review, 2021

Hazard domain	Identified risk	Example
	disruption to critical freight infrastructure and services due to other reasons such as strikes.	payments (due to company restructuring to cope during the pandemic). The combined conditions caused to plan and participate in strikes several times, with some 7,000 striking workers affecting as they protested working conditions[286,287]

Existing legislation related to critical freight assets

Overview of regulation			Identified gaps
Maritime	*Australian Maritime Safety Authority Act 1990 (Cth)*	The main objects of this Act are: (a) to promote maritime safety; and (b) to protect the marine environment; and (c) to promote the efficient provision of services by the Authority.	While the Act may contribute to suitable risk management, explicitly environmental security and protection, it does not amount to an all-hazards approach to risk management, nor is the requirement for a safety management system imposed on a whole-of-sector basis.
	Carriage of Goods by Sea Act 1991	The object of this Act is to introduce a regime of marine cargo liability that: (a) is up-to-date, equitable and efficient; and (b) is compatible with arrangements existing in countries that are major trading partners of Australia; and (c) considers developments within the United Nations in relation to marine cargo liability arrangements.	While the Act may contribute to suitable risk management, including cargo regulations in line with international standards, it does not amount to an all-hazards approach to risk management, nor is the requirement for a safety management system imposed on a whole-of-sector basis.
	Marine Safety Act 2010 (Vic)	The purpose of this Act is to provide for safe marine operations in Victoria through safety rules and regulations pertaining to staff, operation of vessels, licensing, and physical security.	While the Act may contribute to suitable risk management, it does not amount to an all-hazards approach to risk management, nor is the requirement for a safety management system imposed on a whole-of-sector basis.
	Maritime Transport and Offshore Facilities Security Act 2003 (MTOFSA) & Maritime Transport and Offshore Facilities Security Regulations	The purpose of the Act and Regulations is to safeguard against unlawful interference with maritime transport or offshore facilities. To achieve this purpose, this Act establishes a regulatory framework centred around the development of security plans for ships, other maritime transport operations and offshore facilities. The implementation of a	While the legislation and regulations may contribute to suitable risk management, it does not amount to an all-hazards approach to risk management, nor is the requirement for a safety management system imposed

[286] Business News Australia, 2021

[287] ABC News, 2021

Overview of regulation			Identified gaps
	2003 (Cth)	security plan should make an appropriate contribution to the achievement of the maritime security outcomes.	on a whole-of-sector basis and is limited to specific sections of the maritime industry.
	Occupational Health and Safety (Maritime Industry) Act 1993 (Cth) *Occupational Health and Safety (Maritime Industry) (National Standards) Regulations 2003 (Cth)* *Occupational Health and Safety (Maritime Industry) Regulations 1995 (Cth)*	The objects of this Act are: (a) to secure the health, safety and welfare at work of maritime industry employees; and (b) to protect persons at or near workplaces from risks to health and safety arising out of the activities of maritime industry employees at work; and (c) to ensure that expert advice is available on occupational health and safety matters affecting maritime industry operators, maritime industry employees and maritime industry contractors; and (d) to promote an occupational environment for maritime industry employees that is adapted to their health and safety needs; and (e) to foster a cooperative consultative relationship between maritime industry operators and maritime industry employees on the health, safety and welfare of maritime industry employees at work. The object of this Regulation complimenting the Act is to minimise the risk to the health of persons due to exposure to hazardous substances: (a) by regulating hazardous substances used at workplaces, (b) by providing for: (i) the assessment of the risk of exposure to hazardous substances; and (ii) the control of exposure to hazardous substances; and (iii) the training of employees and contractors who could be exposed to hazardous substances at work on the nature of the hazard and the level of risk posed by the hazardous substances, and the means of assessing and controlling exposure to the substances	While the legislation and regulations may contribute to suitable risk management, it does not amount to an all-hazards approach to risk management. The Act and Regulations are primarily centred on safety rather than security, resulting in the legislation focusing primarily on personnel security and does not address a whole-of-sector risk management approach.
	Ports and Maritime Administration Act 1995	The principal objectives of the Act are to increase and maintain business security and resilience, maintain operational security practices and improve efficiency in ports and the port-related supply chain.	While the Act may contribute to suitable risk management, it does not amount to an all-hazards approach to risk management, nor is the requirement for a safety management system imposed on a whole-of-sector basis.
Rail	*Rail Safety National Law* *Rail Safety National Law (South Australia) (Drug and Alcohol Testing) Regulations 2012*	The creation of a single national entity replaced seven separate regulatory authorities. The Rail Safety National Law establishes ONRSR as the body responsible for rail safety regulation in that state or territory. The regulations compliment the Act to define the requirements of personnel in rail operations. This includes rules and regulations, qualifications, and practices.	While the legislation and regulations may contribute to suitable risk management, it does not amount to an all-hazards approach to risk management. They do not address a cyber or supply chain risk management approaches.

Overview of regulation			Identified gaps
Road	*Heavy Vehicle National Law*	The object of this Law is to establish a national scheme for facilitating and regulating the use of heavy vehicles on roads in a way that— (a) promotes public safety; and (b) manages the impact of heavy vehicles on the environment, road infrastructure and public amenity; and (c) promotes industry productivity and efficiency in the road transport of goods and passengers by heavy vehicles; and (d) encourages and promotes productive, efficient, innovative, and safe business practices.	While the law contributes to suitable risk management, it does not amount to an all-hazards risk management approach. Specifically, it lacks a focus on cyber and supply chain risk management nor does it have a holistic approach across physical and personnel risk management.

Existing standards, guidelines and regulators for critical freight assets

	Regulator/s
Commonwealth	ACCC ALC AMSA ARTC ATSB Austroads Comcare Department of Home Affairs Department of Infrastructure, Transport, Regional Development, Communications and the Arts Fair Work Ombudsman IMO ISO National Freight and Supply Chain Strategy NHVR ONRSR Ports Australia RISSB
Australian Capital Territory	WorkSafe ACT
New South Wales	SafeWork NSW
Northern Territory	NT WorkSafe Department of Infrastructure, Planning and Logistics
Queensland	Department of Transport and Main Roads WorkCover Queensland
South Australia	SafeWork SA Department for Infrastructure and Transport
Tasmania	Department of State Growth WorkSafe Tasmania
Victoria	Department of Transport Freight Victoria WorkSafe Victoria

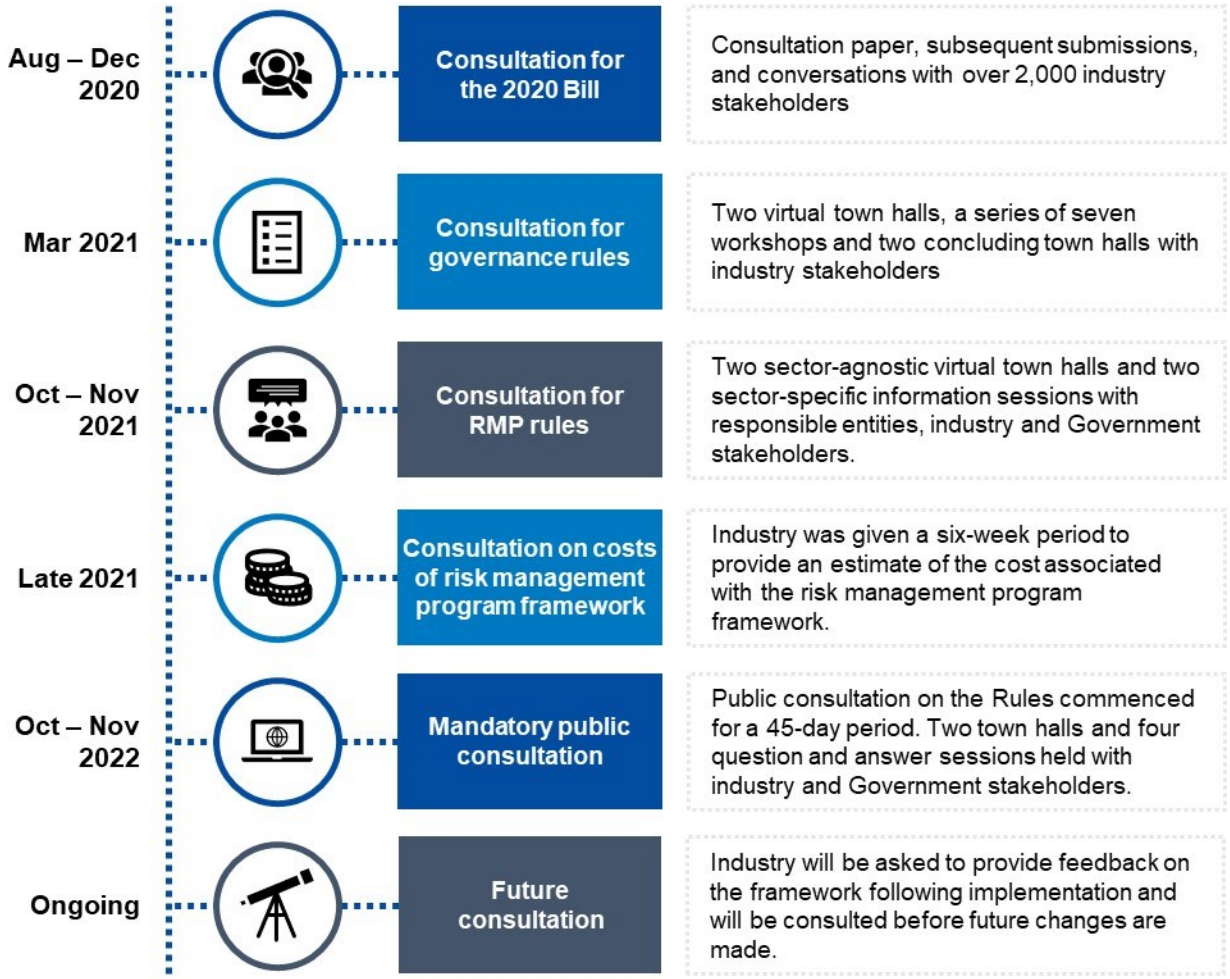
	Regulator/s
Western Australia	WorkSafe WA Arc Infrastructure

Additional information on consultation

Overview of stakeholders consulted

Stakeholders Consulted	
• Australia Post • TasRail • Australian Logistics • VicTrack • Toll Group • Linfox	• Aurizon • NSW Ports • Pacific National • Victoria International Container Terminal • Australian Rail Track Corporation • SCT Logistics

Consultation timeline



RMP Rules consultation

The Department undertook extensive consultation with industry, including the freight infrastructure and services sector for the design of RMP rules, with the objectives of:

- Assessing whether there are existing regulations that meet the Bill's RMP objectives, to ensure the regulatory burden is reduced where possible; and
- Ensuring there are rules in place that will drive an uplift in the security and resilience of critical freight infrastructure and services assets.[288]

Consultation with industry stakeholders occurred across the following key stages:

1. **A virtual Town Hall**, held on 19 October 2021, attended by 360 approximately industry and Government stakeholders, including from the freight infrastructure and services sector. The purposes of the session were to:
    i. Outline the CI/SONS reforms and provide an update on the SLACI Bill (now SLACIP Act) and SLACIP Bill (now SLACIP Act);
    ii. Provide an update for industry on the decision to consult on sector-agnostic RMP rules (as opposed to sector-specific rules), and outline how this would affect the consultation process going forward; and
    iii. Answer any questions about the Bills or RMP rules consultation process.
2. **Two freight-specific Information Sessions,** held on 4 and 24 November 2021, attended by approximately 40 industry and Government stakeholders. The purpose of the information sessions was to reiterate the update for industry on the move from sector-specific to sector-agnostic RMP rules and to gain sector-specific feedback on the RMP rules.
3. **A wrap-up virtual Town Hall** held on 25 November 2021. The purpose of the Town Hall was to present the updated RMP rules and provide information on the further consultation period. The Town Hall was attended by approximately 800 industry and Government stakeholders across the 11 critical infrastructure sectors, including by stakeholders from the freight infrastructure and services asset classes.
4. **Out of session consultation:**
    – Stakeholders were encouraged to contact the Department out of session. The Department availed itself to stakeholders to discuss their concerns, working to ensure stakeholders' understanding of the rules, and the rules' proportionality.
    – Out of session engagement also assisted in the iterative development of rules between workshops, through addressing concerns raised by individual stakeholders and proposing a solution.
    – This engagement strengthened the relationship between the Department and industry, while providing insights on implementation costs, entities' operating environments and the overall impacts of the proposed regulatory changes.
5. **Mandatory Public Consultation**, following the Minister commencing a 45-day consultation period on 5 October 2022 (the mandatory period is 28 days). Consultation included two Town Hall Sessions held on 10 October and 12 October 2022, attended by approximately 550 industry and Government stakeholders (across both sessions). The sessions provided information on the proposed RMP Rules as well as the broader obligation. These Town Halls, as well as four subsequent question and answer sessions, provided an opportunity for industry to ask questions about the proposed RMP Rules and process.

[288] Department of Home Affairs 2021, p. 2

Outcomes and themes from consultation on RMP rules

Key themes from consultation

Rule category	Identified themes		Impact on development of rules
RMP Rules	**Information sessions**	• There is an **appetite for guidance material** to support sector-specific uplift in security and resilience.	In response to feedback received during the information sessions, the Department committed to: • The development of guidance materials, which would highlight aspects of risk management that should be prioritised by responsible entities and assist industry in interpreting and implementing the rules to achieve an uplift in security and resilience.

Consultation on costs

During the second information session, attendees were invited to participate in cost impact data collection through the completion of a cost impact template. This template was designed to collect substantive costing data to supplement the anecdotal costing discussions which had occurred throughout the workshop series. Industry were asked to provide:

- Their demographic information;
- Effort and cost estimates split by one-off and ongoing costs, staff effort, capital and other operating costs, and an estimated range between expected costs and highest possible costs; and
- Any comments on key boundaries, assumptions and cost drivers attached to the costing estimates provided.

Industry was provided with the template on 24 November 2021, with submissions open for a period of four weeks and closing on 22 December 2021.

The absence of entities within the sector that meet the definition of a small business indicated that consultation with the Australian Small Business and Family Enterprise Ombudsman was not required to identify expected costs to small businesses in preparing this RIS.[289]

[289] Office of Best Regulation Practice, 2021

Appendix R: Supplementary information for critical food and grocery assets

Overview of the role of food and grocery assets in Australia

The food and grocery sector in Australia is large and complex, comprised of a range of businesses up and down the supply chain. The sector includes food manufacturing, processing, packaging, distributing, and supplier businesses – ranging in scale from small family-owned operations to large multi-national corporations across Australia. These businesses produce and distribute a wide range of goods from food and beverage to non-food grocery products such as personal care products (over-the-counter medicines, toothpaste, skin lotions, cosmetics, toilet tissues), house care products (cleaning products, insecticides), pet care products, and numerous other miscellaneous items.[290]

This sector plays an important role in ensuring the wellbeing of Australian citizens by facilitating access to essential food and groceries. In Australia, the grocery retail sector is dominated by four main retailers who account for 80% of the market: Woolworths (37.1%), Coles (29%), Aldi (9.5%) and Metcash (6.9%).[291] Metcash's retail brands include IGA, Supa IGA (supermarkets) IGA X-press (convenience stores), IGA Fresh, Foodland and Friendly Grocer. The remaining supermarket sector is made up of providers with small retail footprints such as Costco and Amazon.[292]

The food and grocery wholesaling industry is generally divided into two groups – wholesalers who supply food retailers and wholesalers who supply food services. Food retailers are predominantly grocery stores, which require staple dry goods, toiletries, and fresh produce, whereas food services also require food items that are partly prepared, allowing businesses to reduce preparation time. The major players, which account for over 50% of the market, cater to both groups – see Metcash (41.1%), PFD Foods (9%) and Bidfoods (8.6%).[293]

However, for the purposes of the SOCI Act, the critical food and grocery assets have been defined to only include essential food and grocery services. Section 12K of the SOCI Act provides the following in relation to 'critical food and grocery asset'.

*(1) An asset is a **critical food and grocery asset** if it is a network that:*

(a) is used for the distribution or supply of:

(i) essential food; or

(ii) essential groceries; and

(b) is owned or operated by an entity that is:

(i) a critical supermarket retailer, in accordance with subsection (2); or

(ii) a critical food wholesaler, in accordance with subsection (3); or

(iii) a critical grocery wholesaler, in accordance with subsection (4).

Note: The rules may prescribe that a specified critical food and grocery asset is not a critical infrastructure asset (see section 9).

---

[290] https://www.homeaffairs.gov.au/reports-and-pubs/files/critical-infrastructure-consultation-submissions/EDS010-CISoNS-AustralianFoodandGroceryCouncil.PDF

[291] IbisWorld, *Supermarket & Grocery Stores In Australia, Industry Report G4111,* March 2022.

[292] IbisWorld, *Supermarket & Grocery Stores In Australia, Industry Report G4111,* March 2022.

[293] Ibid.

(2) For the purposes of subparagraph (1)(b)(i), the rules may prescribe:

(a) specified entities that are critical supermarket retailers; or

(b) requirements for an entity to be a critical supermarket retailer.

(3) For the purposes of subparagraph (1)(b)(ii), the rules may prescribe:

(a) specified entities that are critical food wholesalers; or

(b) requirements for an entity to be a critical food wholesaler.

(4) For the purposes of subparagraph (1)(b)(iii), the rules may prescribe:

(a) specified entities that are critical grocery wholesalers; or

(b) requirements for an entity to be a critical grocery wholesaler.

Under the SOCI Act, the Government may create rules that prescribe an asset to be a critical infrastructure asset. Under the Security of Critical Infrastructure (Definitions) Rules (LIN 21/039) 2021 – which came into effect in March 2022 –Aldi Pty Limited, Coles Group Limited, and Woolworths Group Limited were prescribed as a *critical supermarket retailer* and MetCash Trading Limited prescribed as a *critical grocery wholesaler*.

Impacts of a disruption to critical food and grocery assets

The consequences of a prolonged and widespread disruption to a critical food and grocery asset may include:

- Disruption to access to essential food stuffs for households.
- Disruption to access to essential food products and over the counter health products for vulnerable people and communities.
- Reduced choice or increased cost of food products for consumers.
- Disruption to commercial food services.
- Disruption to the centralised distribution and food processing model.
- Breach of privacy and customer data.
- Inability for businesses to function as normal.

Examples of disruptions to food and grocery assets – domestic and international

Past incidents, both in Australia and overseas, demonstrate the potentially severe, cascading consequences of prolonged disruption in any critical infrastructure sector – for that sector itself, for other critical infrastructure sectors, and for the affected national economy. The following series of case studies, each categorised by its relevant hazard domain or domains, demonstrate these consequences, in the context of critical food and grocery assets. While some are drawn from overseas, these case studies highlight a clear imperative for decisive action, in order to prevent the occurrence of similar, or further, incidents for Australia's critical food and grocery assets.

Coop Supermarket closures (2021)	**Cyber security**
Situation: In 2021, more than half of all Coop Supermarkets in Sweden were forced to close for nearly a week as the result of a cyber-attack. Point of sales tills and self-service checkouts stopped working as a result of an attack on a third-party software provide, Kaseya. Media reports suggest that a $92 million	

ransom request was made to the third-party software provider Kaseya for the release of stolen data.[294]

Outcome: Around 500 supermarkets were closed for nearly a week, reducing consumer access and choice for fresh food and grocery produce. Kaseya announced it had received a universal decryptor tool for the REvil-encrypted files from an unnamed "trusted third party" and was helping victims restore their files. It is suggested that the cost of this breach and consequent closure of stores cost Coop AUD$28 million.[295]

Identified Gap: This attack highlights the underlying vulnerability within the cyber security domain.

JBS meat processing ransomware attack (2021)	Cyber security

Situation: JBS Foods Group, is the world's largest meat processing company, supplying one-fifth of meat globally, with a global footprint including Australia. JBS US Headquarters was the target of an organised cybersecurity attack, affecting some of the servers supporting its North American and Australian IT systems. The company took immediate action, suspending all affected systems, notifying authorities and activating the company's global network of IT professionals and third-party experts to resolve the situation.[296]

Outcome: JBS Foods Group closed all of its beef processing plants in the US, Canada and Australia, resulting in over 7000 employees being temporarily stood down in Australia alone. JBS Food Groups paid the equivalent of $US11 million ($14.2 million) to a criminal gang to end a five-day cyber attack.[297]

Identified Gap: This attack highlights the underlying vulnerability within the cyber security domain.

Food shortages in the Northern Territory & Western Australia due to flooding in South Australia (2022)	Physical & natural hazard

Situation: In January 2022, significant rains occurred resulting in rail and road links connecting Adelaide to Darwin becoming flooded resulting in freight vehicles not being able to bring in fresh food and groceries into the Northern Territory.[298] The flooding event also washed out 300km of the only rail line that supplies WA with food and essential goods from Australia's eastern states creating acute shortages of essential items.[299] Rail freight accounts for 80% of land transport into WA and took 25 days to reopen.[300]

Outcome: Many supermarkets introduced purchase limits and re-routed freight from their east coast distribution hubs through much longer routes to try and bring in basic supplies. Food distributors in WA were forced to dump thousands of tonnes of perishable items (e.g. dairy, meat) and alternative transport costs rose steeply with these costs passed onto the consumer. For example, the cost to hire one-way flatbed semi-trailer doubled from $6,000 to $12,000 during this period. Rural and remote communities faced food shortages and food distress.[301] Road transport of goods – the primary mode of fresh produce supply into NT – from Adelaide distribution centres completed a 3000km detour via Queensland to reach NT retailers.[302]

[294] https://www.abc.net.au/news/2021-07-06/hackers-demand-92m-after-gargantuan-ransomware-attack/100269678

[295] https://www.statista.com/statistics/1063165/revenue-of-coop-retail-stores-in-sweden-by-region/

[296] https://jbsfoodsgroup.com/articles/jbs-usa-cyberattack-media-statement-june-9

[297] https://www.abc.net.au/news/rural/2021-06-10/jbs-foods-pays-14million-ransom-cyber-attack/100204240

[298] https://www.afr.com/companies/infrastructure/rail-and-road-flooding-intensifies-supply-chain-crisis-20220131-p59sk3

[299] https://www.theguardian.com/australia-news/2022/feb/04/a-logistical-nightmare-flooding-takes-out-sole-rail-link-sparking-west-australian-food-shortage

[300] https://www.abc.net.au/news/2022-02-15/nt-rail-link-reopens-25-days-after-flood-damage/100824484

[301] https://www.afr.com/companies/infrastructure/rail-and-road-flooding-intensifies-supply-chain-crisis-20220131-p59sk3

[302] https://www.theguardian.com/australia-news/2022/feb/04/a-logistical-nightmare-flooding-takes-out-sole-rail-link-sparking-west-australian-food-shortage

Identified Gap: Limitations in local food supply chains mean that populations are reliant on interstate and international supply chains for access to food and groceries.

Food shortages in North & West Queensland due to floods in South East Queensland & Northern NSW (2022)	**Physical & natural hazard**

Situation: A low pressure system caused a rain event that inundated South East Queensland and Northern NSW cutting off freight and rail access to regions north of Gympie (QLD) and south of Grafton (NSW). Major distribution centres and warehouses were inundated by flood waters and highways connecting the east coast were impacted, leaving trucks carrying fresh produce stranded.[303] Shortages and product limits were imposed due to a combination of transport corridor interruptions, loss of primary production for certain goods concentrated in the flood affected areas, and major distribution centres unable to operate.[304] Additionally, a freight train derailment near Gympie (QLD) cut rail freight access to regions isolated due to road closures (also highlighting the interconnected nature of critical infrastructure).

Outcome: Hundreds of major supermarket stores were closed as a direct result of flooding. Regional areas (outside the flood-affected zones) were unable to access fresh food and groceries for a number of days. Retailers were unable to source goods and were forced to close or operate with minimal stock of essential items which had knock-on effects to other local businesses who source fresh produce from these local centres.[305] Major supermarkets introduced state-wide purchase limits to manage a critical shortage of products, including fresh milk, still water, toilet paper and meat.[306]

Identified Gap: Limitations in local food supply chains mean that populations are reliant on interstate and international supply chains for access to food and groceries. Concentration of food production in central areas and major distribution hubs creates reliance on supply flows through critical nodes for dispersed populations across regional areas.

Labour shortages due to COVID in food processing, distribution and retail (2022)	**Personnel & supply chain hazard**

Situation: Labour shortages due to high COVID infection rates and mandated isolation periods across Australia reduced supply capacity for food processing, distribution and retailers. Similar trends were seen around the world at the peak of the crisis. Supply capacity sharply declined and caused major shortages and price increases. During the period some meat processing companies were operating with half their required staff.[307] The Australian Meat Industry Council indicated some meat production businesses had less than 30% of workers available for regular shifts.[308] Supply disruptions due to labour shortages were also noticeable for food distributors and retailers. Absenteeism at Woolworths distribution centres ranged from 20-40%, while Coles estimated 10% of retail staff were affected – figures echoed across the sector.

Outcome: Shortage of meat products and backlog of agricultural inputs. Increased prices due to scarcity of certain types of processed goods and additional transport costs. The sharp decrease in processing capacity had flow-on effects to downstream suppliers of agricultural inputs in managing excess stock. The compounding effect of livestock backlog imposes additional costs such as a decline in animal welfare due to overcrowding, extended shelter and feed costs, animal destruction, and psychological trauma on producers. [309] [310] [311]

[303] https://www.theguardian.com/australia-news/2022/mar/02/nothing-to-sell-queensland-and-nsw-flood-waters-hit-supermarket-grocery-supplies

[304] https://www.theguardian.com/australia-news/2022/mar/02/nothing-to-sell-queensland-and-nsw-flood-waters-hit-supermarket-grocery-supplies

[305] https://www.theguardian.com/australia-news/2022/mar/02/nothing-to-sell-queensland-and-nsw-flood-waters-hit-supermarket-grocery-supplies

[306] https://www.afr.com/politics/floods-damage-bill-set-to-top-2b-20220302-p5a0z5

[307] https://www.abc.net.au/news/rural/2022-01-11/chicken-shortage-due-to-covid-staff-shortage-in-meat-processing/100749802

[308] https://amic.org.au/domestic-meat-shortages-loom-as-processors-face-covid-induced-labour-shortage/

[309] https://committees.parliament.uk/publications/9580/documents/162177/default/

Identified Gap: Limitations in local food supply chains mean that populations are reliant on interstate and international supply chains for access to food and groceries.

Closure of Supermarkets in South Coast NSW due to bushfires (2020)	Personnel, physical & natural hazard
Situation: Bushfires devastated the South Coast of New South Wales (NSW) in the summer of 2020 and caused widespread disruption due to the dangerous conditions. Woolworths chose to close some of its stores for short periods to deal with loss of electricity infrastructure, personnel shortages and inability of supply to reach retailers.[312] Fire and smoke hazards closed roads, damaged food stocks and prevented movement of essential items.[313]	
Outcome: Local residents were unable to purchase fresh food and groceries for a number of days.[314] Medium-term effect on price and availability on perishable goods.	
Identified Gap: Limitations in local food supply chains mean that populations are reliant on interstate and international supply chains for access to food and groceries.	

Baby formula shortage in the US (2022)	Personnel & supply chain hazard
Situation: In early 2022, many supermarkets and other point of sale outlets in the US were unable to stock sufficient levels of baby formula to meet consumer demands. This shortage was a result of the closure of one domestic manufacturing facility, strict importing regulations, highly concentrated domestic industry and COVID related supply chain challenges.[315]	
Outcome: There was a shortage of 40% of baby formula in the US market with certain states and regions more affected (some greater than 90%).[316] To resolve the issue, President Biden invoked the Defense Production Act to increase domestic production. President Biden also launched 'Operation Fly Formula' to fly in formula from overseas and Congress passed legislation to temporarily suspend import tariffs.[317] However, gaps in supply will persist until strategic changes are adopted in the policy settings and domestic production systems.	
Identified Gap: Domestic standards are inconsistent with some international standards making importing supply on need harder. Market concentration can impact when key facilities are not operational.	

Key risks to critical food and grocery assets

Hazard domain	Identified risk	Example
Physical & Natural	Despite the rise of online delivery, shop storefronts and distribution centres remain	In early 2020, bushfires on the South Coast of NSW meant that supermarkets were closed as

[310] https://www.bbc.com/news/uk-northern-ireland-58637030
[311] https://www.stuff.co.nz/southland-times/128309125/meatworks-losing-millions-in-valueadded-products
[312] https://www.smh.com.au/business/companies/bushfires-likely-to-impact-australian-retailers-analysts-say-20200108-p53pqi.html
[313] https://www.theguardian.com/australia-news/2020/jan/17/australias-bushfires-could-affect-cost-and-availability-of-fresh-local-produce
[314] Ibid
[315] https://www.pbs.org/newshour/economy/how-the-baby-formula-shortage-financially-strains-u-s-families
[316] https://www.cnbc.com/2022/05/09/40-percent-of-americas-baby-formula-supplies-are-out-of-stock.html
[317] https://www.pbs.org/newshour/economy/how-the-baby-formula-shortage-financially-strains-u-s-families

Hazard domain	Identified risk	Example
Hazard	key for access to food and groceries.	a result of lack of power, lack of staff and lack of capacity to receive groceries. This resulted in local communities not to have access to fresh foods.
Cyber	Supermarkets and wholesalers are increasingly utilising technology across all areas of service including point of sale, stock management, merchandising, staffing and finance, data and sales increasing the points of vulnerability.	In 2020, Coles, was hit by an IT outage for a little over four hours and forced to shut its outlets, with shoppers unable to complete purchases due to an inability to process payments.
Supply Chain	The physical supply chain has presented difficulties, in particular during the COVID-19 pandemic. This is because of its unique market conditions in which local supply chains are highly concentrated between the two main supermarket players and one large wholesaler, limited local manufacturing and production and distribution centres a significant distance from supermarkets.[318] In addition, Australia relies on international supply chains to fill gaps in domestic production which is subject to a range of externalities.	The COVID-19 pandemic and natural disasters have highlighted concerns regarding the vulnerability of Australia's food supply chain exposing many people to short term food and grocery shortages.
Personnel	When personnel are unable to operate due to events beyond their control, to personnel shortages within the supply chain. Additionally, employees having access to systems, data, or premises may offer insider threat concerns such as fraud, theft, intelligence, infrastructure sabotage, and data misuse.	An employee stole the personal data of employees of Morrison supermarket (UK) and posted the data online causing distress to its staff.[319]

Existing legislation related to critical food and groceries assets

Overview of regulation		Identified gaps
Australian Competition & Consumer Commission (ACCC)	The *Competition and Consumer Act 2010* (CCA) covers most areas of the market: the relationships between suppliers, wholesalers, retailers, and consumers. Its purpose is to enhance the welfare of Australians by promoting fair trading and competition, and through the provision of consumer protections. Broadly, the CCA covers: • product safety and labelling	The ACCC, through the CCA and related Regulations, provides a framework for the regulation of relationships and commercial dealings between retailers, wholesalers and suppliers. However, this framework does not regulate risk management for cyber security incidents and reporting, to avoid disruptions to food and grocery services and supply chain, and wider supply chain issues.

[318] https://lighthouse.mq.edu.au/article/january-2022/more-supermarket-diversity-would-ease-supply-disruptions

[319] https://www.theguardian.com/business/2020/apr/01/morrisons-is-not-liable-for-massive-staff-data-leak-court-rules

Overview of regulation		Identified gaps
	• unfair market practices • price monitoring • industry codes • industry regulation – airports, electricity, gas, telecommunications mergers and acquisitions	
	The *Competition and Consumer (Industry Codes – Food and Grocery) Regulation 2015* is made under s 51AE of the CCA. The Regulation prescribes the voluntary *Food and Grocery Code of Conduct,* which aims to: • regulate standards of business conduct to sustain cooperation and trust; • ensure transparency and certainty in commercial transactions; • provide equitable dispute resolution processes arising between retailers, wholesalers and suppliers; and • promote and support good faith commercial dealings.	
Food Standards	Food Standards Australia and New Zealand (FSANZ) is a statutory authority established under *Food Standards Australia New Zealand Act 1991*, which: • develops and manages standards for food, called the Food Standards Code • regulates labelling that goes on packaged and unpackaged food, including warnings and advisory labels • manages food recalls	Whilst providing standards for food, including labelling, these do not specifically include requirements to reduce cyber security, supply chain and personnel hazards.
Import requirements	The *Commerce (Trade Descriptions) Act 1905* (the Act) and the Commerce (Trade Descriptions) Regulation 2016 (the Regulation) set out which goods or classes of goods require labelling when being imported into Australia, what label is required and where the label must be applied.	Creates requirements for imported good to meet standards, including for labelling for goods being imported to Australia. These do not specifically include requirements to reduce cyber security, supply chain and personnel hazards.
Food Safety and Regulations	The Australian Government and state and territory governments enforce the standards, in line with their food legislation.	While these regulatory frameworks have some risk management features relating to food safety and quality, they do not include requirements to reduce cyber security, supply chain and personnel hazards.

Existing standards, guidelines and regulators for critical food and grocery assets

Hazard domain	Organisation	Standards & guidelines
Cyber	National Institutes of Standards and Technology (NIST)	**Cybersecurity Programs**
	International Organization for Standardization (ISO)	**ISO 27001** provides requirements for information security management systems.
Physical	Standards and codes for Supermarkets	Food and Grocery Code – a voluntary code prescribed under the Competition and Consumer Act 2010 (CCA). It was introduced to improve standards of business conduct in the food and grocery sector. The Australian Government and state and territory governments enforce the standards, in line with their food legislation.
	Standards and codes for essential food items	Primary Production and Processing Standards which includes seafood, dairy, poultry meat, meat and meat products, eggs and egg products and seed sprouts.

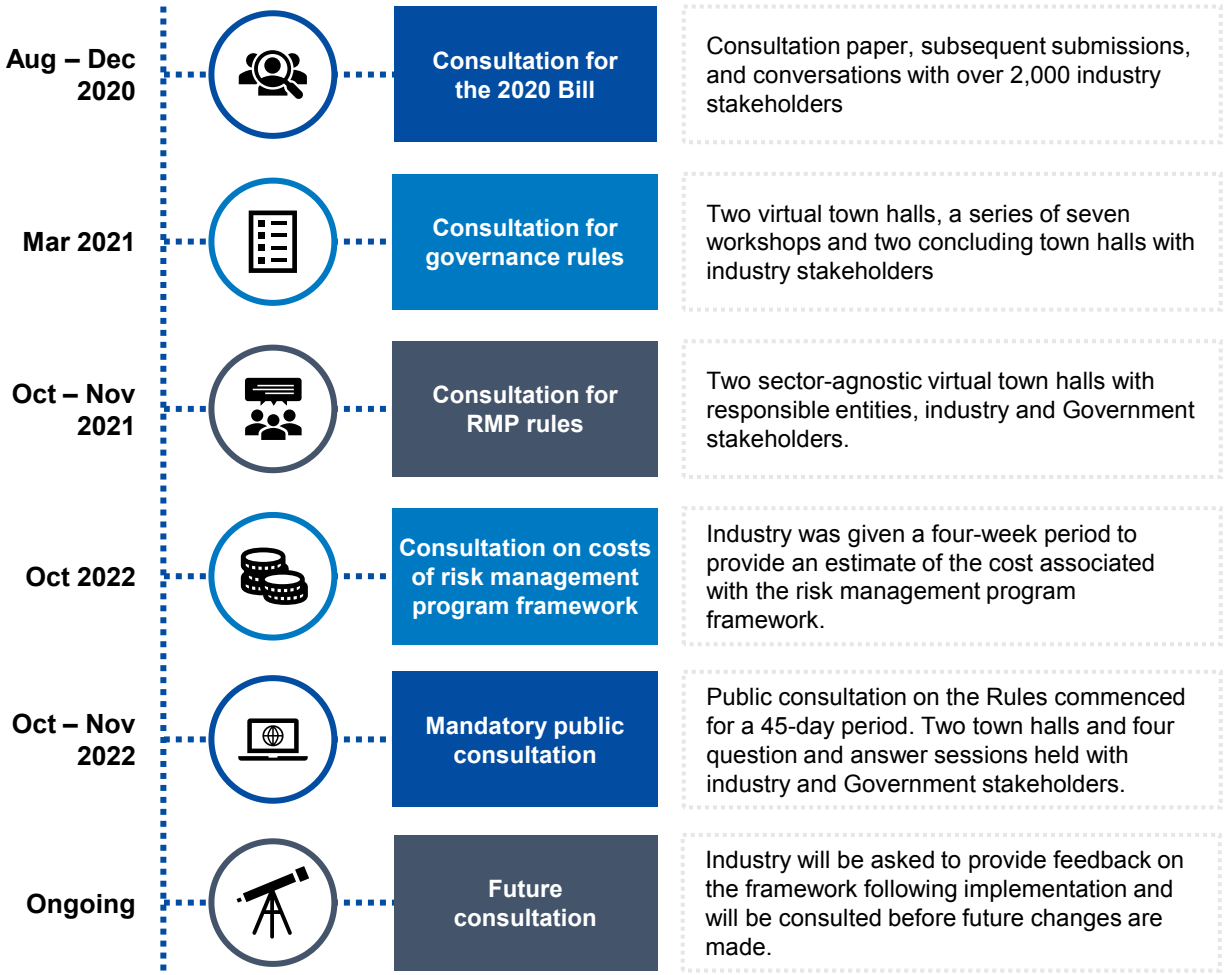
Jurisdiction	Regulator/s
Commonwealth	Australian Competition and Consumer Commission (ACCC), which regulates relationships between suppliers, wholesalers, retailers, and consumers. Department of Agriculture, Fisheries and Forestry, which enforces the Food Standards Code on imported foods. The Australian Pesticides and Veterinary Medicines Authority (APVMA), which is responsible for approving agricultural and veterinary chemicals for use.
State and Territory Jurisdictions	Each state and territory has a legislative framework which prescribes food and grocery standards, regulates licensing arrangements and prescribes compliance activities regarding food quality and safety.
Australian Capital Territory	Health Protection Service
New South Wales	NSW Food Authority
Northern Territory	Department of Health
Queensland	Queensland Health – Food Safety Standards and Regulation Safe Food Queensland (primary production and processing)
South Australia	SA Health Department of Primary Industries and Regions SA Dairy Authority of South Australia
Tasmania	Department of Health and Human Services – Food Safety Department of Primary Industries, Parks, Water and Environment Tasmanian Dairy Industry Authority
Victoria	Department of Health and Human Services

Additional information on consultation

Overview of stakeholders consulted

Stakeholders Consulted	
• Woolworths	• ALDI
• Coles	• Metcash

Consultation timeline



RMP Rules consultation

The Department undertook extensive consultation with industry, including the food and grocery sector for the design of RMP rules, with the objectives of:

- Assessing whether there are existing regulations that meet the risk management program objectives, to ensure the regulatory burden is reduced where possible; and
- Ensuring there are rules in place that will drive an uplift in the security and resilience of critical food and grocery assets.

Consultation with industry stakeholders occurred across the following key stages:

1. **A virtual Town Hall**, held on 19 October 2021, attended by 360 approximately industry and Government stakeholders, including from the food and grocery sector. The purposes of the session were to:

    i. Outline the CI/SONS reforms and provide an update on the SLACI Bill (now SLACI Act) and SLACIP Bill (now SLACIP Act);

    ii. Provide an update for industry on the decision to consult on sector-agnostic RMP rules (as opposed to sector-specific rules), and outline how this would affect the consultation process going forward; and

    iii. Answer any questions about the Bills or RMP rules consultation process.

2. **A wrap-up virtual Town Hall** held on 25 November 2021. The purpose of the Town Hall was to present the updated RMP rules and provide information on the further consultation period. The Town Hall was attended by approximately 800 industry and Government stakeholders across the 10 critical infrastructure sectors, including by stakeholders from the food and grocery sector.

3. **Out of session consultation**:

    - Stakeholders were encouraged to contact the Department out of session. The Department availed itself to stakeholders to discuss their concerns, working to ensure stakeholders' understanding of the rules, and the rules' proportionality.
    - Out of session engagement also assisted in the iterative development of rules between workshops, through addressing concerns raised by individual stakeholders and proposing a solution.
    - This engagement strengthened the relationship between the Department and industry, while providing insights on implementation costs, entities' operating environments and the overall impacts of the proposed regulatory changes.

4. **Mandatory Public Consultation**, following the Minister commencing a 45-day consultation period on 5 October 2022 (the mandatory period is 28 days). Consultation included two Town Hall Sessions held on 10 October and 12 October 2022, attended by approximately 550 industry and Government stakeholders (across both sessions). The sessions provided information on the proposed RMP Rules as well as the broader obligation. These Town Halls, as well as four subsequent question and answer sessions, provided an opportunity for industry to ask questions about the proposed RMP Rules and process.

Outcomes and themes from consultation on RMP rules

Key themes from consultation

Rule category	Identified themes		Impact on development of rules
RMP Rules	**Information sessions**	• The food and grocery sector **broadly agrees** with the RMP rules as drafted. • The food and grocery sector currently has various levels of risk maturity. • There is an **appetite for guidance material** to support sector-specific uplift in security and resilience, especially with regards to meeting the supply chain rules.	In response to feedback received during the information sessions, the Department committed to: • The development of guidance materials, which would highlight aspects of risk management that should be prioritised by responsible entities and assist industry in interpreting and implementing the rules to achieve an uplift in security and resilience.

Consultation on costs

Specific sessions were held with the food & grocery sector (on 12 and 13 October 2022) where participants were provided with an overview of the Rules and attendees were invited to participate in cost impact data collection through the completion of a cost impact template. This template was designed to collect substantive costing data to supplement the anecdotal costing discussions which had occurred throughout the workshop series. Industry attendees were asked to provide:

- Their demographic information;
- Effort and cost estimates split by one-off and ongoing costs, staff effort, capital and other operating costs, and an estimated range between expected costs and highest possible costs; and
- Any comments on key boundaries, assumptions and cost drivers attached to the costing estimates provided.

Industry was provided with the template on 13 October 2022, with submissions open for a period of four weeks and closing on 10 November 2022.

The absence of entities within the sector that meet the definition of a small business indicated that consultation with the Australian Small Business and Family Enterprise Ombudsman was not required to identify expected costs to small businesses in preparing this RIS.[320]

[320] Office of Best Regulation Practice, 2021

Appendix S: Detailed costing information for critical electricity assets

Costing process completed by responsible entities for critical electricity assets

Cost submissions were received from 27 responsible entities for critical electricity assets. This represented approximately 49% of the market share within this critical infrastructure asset class.

The market share percentage of responsible entities who made a submission was calculated using entity and electricity business type (that is, transmitter, generator or distributor) data sourced from IBISWorld. The market share of submissions was first determined at an electricity business type level by summing the business type market share percentage. The market share of submissions at each individual business type level was then used to extrapolate the total critical electricity assets market share represented by submissions.

To extrapolate the costs of compliance to all critical electricity assets, organisations were categorised firstly by size into 'large' and 'small' entities and then by business type (transmitter, generator or distributor)[321] based on the following definitions:

- 'Large' entity - any entity with greater than 5% of critical electricity assets' revenue in each business type (transmitter, generator or distributor).
- 'Small' entity - any entity with less than 5% of critical electricity assets' revenue in each business type (transmitter, generator or distributor).

Critical electricity asset cost impact submissions broken down by size and business type

Business type	Organisation size	Number of submissions
Transmitters[322]	Large (>5% market share)	5
	Small (<5% market share)	n/a*
Distributors[323]	Large (>5% market share)	3
	Small (<5% market share)	4
Generators[324]	Large (>5% market share)	3
	Small (<5% market share)	12
Total		**27**

***Note:** No cost submissions were received from transmitters with <5% market share.

Likely net benefit – option 2

The following section details the costs and benefits associated with option 2 (the regulatory option), before assessing the overall likely net benefit presented by this option.

[321] An assumption has been made that the distribution of critical electricity assets across responsible entities is the same as the market share allocations across generators, transmitters and distributors.

[322] IBISWorld(a), 2021

[323] Ibid.

[324] IBISWorld(b), 2021

Costs of option 2

There are multiple factors affecting the regulatory burden for each entity, including their existing risk management practices and capabilities, the nature of the critical electricity assets they operate and the size of their operations. In collecting cost information from entities across critical electricity assets, this variance in cost impact has been captured and reflected in the estimates of total cost across critical electricity assets included in this RIS.

When estimating the cost of compliance with option 2, critical electricity asset entities provided both an expected and a high-cost estimate. The high-cost estimate was provided as a way to measure the uncertainty associated with their estimates and the highest feasible cost of option 2. The expected estimate was used as the basis for determining the net benefit of option 2 in section 4.

Using the expected and the high estimate as a range, the cost of compliance is as follows:

- A one-off regulatory cost of between $463.3 (expected) and $758.2 million (high estimate), across critical electricity assets nationally; and
- An ongoing cost of between $228.0 (expected) and $366.4 million (high estimate) per year, across critical electricity assets nationally.

The cost of regulation will be borne by entities responsible for critical electricity assets who meet the relevant thresholds. Community organisations and individuals will not be directly affected but there will likely be indirect costs passed onto consumers. For the purposes of this RIS, the cost of regulation in the table below will only include the initial costs associated with regulation.[325] The indirect cost to consumers and communities has been addressed in the economic analysis through consideration of indirect cost to the wider economy as a result of the proposed risk management program framework.

The average cost of compliance for each entity is estimated at $8.1 million in one-off costs and $3.8 million per year in ongoing costs, noting that there is a wide range provided in submissions from industry. Entity costs range between $0.8 million and $75.5 million in one-off costs and $0.4 million and $61.5 million in on-going costs per year. There are a number of reasons for this range in cost including the size of the entity and the maturity of existing RMPs.

Regulatory cost estimate

Cost Type	Costs ($ million)			
	Business	Community	Individuals	Total cost ($ million)
One-off	463.3 to 758.2	nil	nil	463.3 to 758.2
Ongoing (per year)	228.0 to 366.4	nil	nil	228.0 to 366.4

Note: There will be no direct costs to individuals and communities although price rises may reflect the increased cost of operations as a result of the proposed Risk Management Program framework.

Based on the industry submissions made during consultations, expected total regulatory costs will be highest for rules and obligations associated with addressing supply chain hazards. These costs represent approximately 24.8% of the total cost of implementing the risk management program framework. The cost associated with physical hazards (24.2% of total cost), material risk rules (14.6% of total cost) and cyber-security hazards (13.8% of total cost) are less significant but remain material. Compliance costs associated with legislative obligations, general rules, personnel hazard rules and natural hazard rules were the least costly aspects of the risk management

[325] Department of Prime Minister and Cabinet, 2020

program framework, representing in total approximately 22.6% of costs in total. The total regulatory cost by rule/obligation is set out in the table below.

Following the original discussions with the sector from April 2021 culminating in the development of electricity sector rules and the submission of costs from Industry, it was determined that the sector agnostic RMP Rules would provide greater clarity and ensure greater consistency across all sectors. The Department confirmed with industry that no additional costings would be requested on the updated RMP Rules, as they were either similar to the previously costed rules or a specific rule had been removed. For the purpose of the above estimate of regulatory burden, the original cost submissions provided by industry were used with the removed rules excluded.

Regulatory burden estimate by rule and obligation for critical electricity assets nationally

Rule / obligation	Costs (Expected to High)			
	One-off ($ million)	Ongoing (per year, $ million)	Total cost over 10 years ($ million) [326]	Expected estimate as percentage of total (%)
Risk management program obligations in the Act	26.5 to 46.4	25.0 to 41.0	251.9 to 415.4	9.8
General rules	14.2 to 22.5	4.3 to 9.1	53.0 to 104.8	2.1
RMP Rules				
Cyber and information security hazard	53.3 to 98.5	35.7 to 61.8	356.7 to 654.8	13.8
Personnel hazard	20.8 to 37.0	21.5 to 30.4	225.1 to 310.4	8.7
Supply chain hazard	136.6 to 169.8	53.0 to 77.5	639.9 to 867.6	24.8
Physical hazard	129.3 to 240.0	52.0 to 81.4	623.2 to 972.7	24.2
Natural hazard	6.9 to 12.1	4.8 to 13.1	52.4 to 130.1	2.0
Material risk	75.6 to 131.9	31.7 to 52.0	376.7 to 600.2	14.6
Total critical electricity assets	**463.3 to 758.2**	**228.0 to 366.4**	**2,578.9 to 4,055.8**	**100.0**

Analysis of industry submissions on cost impacts indicate that the expected burden of regulation will be shared across the three business types. The table below shows that transmitters will incur 36.0% of total critical electricity assets compliance costs, generators 30.8% of total costs, distributors 33.2% of total costs.

Large industry participants (being businesses comprising more than 5% total market share) will incur approximately 69.6% of the total regulatory burden compared to 30.4% for small participants (being businesses comprising less than 5% total market share).

Total regulatory burden over 10 years by size and business type for critical electricity assets nationally

Business Type	10- year costs (Expected to High)			
	Large entities by market share ($ million)	Small entities by market share ($ million)	Total ($ million)	Expected estimate as percentage of total costs (%)

[326] For the purposes of calculating a total 10 year cost of compliance with the risk management program framework, ongoing costs were assumed to commence in the year after the required implementation date (for example, for a rule requiring implementation within 2 years, the ongoing costs associated with the rule were assumed to start in year 3 of the 10 year period).

Transmitters	928.1 to 1,105.1	N/A	928.1 to 1,105.1	36.0
Generators	339.6 to 571.8	454.5 to 805.6	794.0 to 1,377.4	30.8
Distributors	527.9 to 1,107.6	328.9 to 465.8	856.8 to 1,573.3	33.2
Total critical electricity assets	**1,795.6 to 2,784.4**	**783.3 to 1,271.4**	**2,578.9 to 4,055.8**	**100.0**

***Note:** No cost submissions were received from transmitters with <5% market share.

The table below compares the share of regulatory cost to market share by entity size and by business type. Large generators and large distributors incur a slightly smaller proportion of cost than their market share.

Distribution of expected regulatory cost compared to market share by entity size and business type

Business Type	Costs and market share			
	Large entities by market share		Small entities by market share	
	% of cost	Market share (%)	% of cost	Market share (%)
Transmitters	100.0*	99.9	0*	0.1
Generators	42.8	47.1	57.2	52.9
Distributors	61.6	76.9	38.4	23.1

***Note:** There is no information on the cost to small transmitters, as no cost submissions were received from small transmitters. The total regulatory cost for transmitters has been allocated to the large transmitters that make up 99.9 per cent of the market share.

The industry submissions also indicated the type of expenditure expected to be incurred. The allocation of expected cost between labour effort, capital and supplier costs is provided in the table below. The analysis shows that 72.6% of one-off costs and 19.4% of ongoing costs are expected to be invested in capital. A relatively small share of costs are associated with labour effort (7.5% of one-off costs and 12.6% of ongoing costs) with operating costs being the largest component of ongoing costs (68.0% of total ongoing costs).

Expected one-off and ongoing costs by cost type for critical electricity assets nationally

Cost Type	Costs (Expected)			
	One-off ($ million)	One-off (%)	Ongoing (per year)	Ongoing (%)
Labour effort	34.7	7.5	28.8	12.6
Capital	336.2	72.6	44.2	19.4
Operating	92.3	19.9	155.0	68.0
Total critical electricity assets	**463.3**	**100.0**	**228.0**	**100.0**

Several industry stakeholders advised that due to the broad nature of the reforms and the uncertainty associated with implementation of the proposed risk management program framework, cost estimates may have been inflated to allow for a worst-case cost impact.

Benefits of option 2

A reliable continuous electricity supply is central to Australia's prosperity. Further, disruption to supply can be a significant cost to the economy. The risk management program framework aims to reduce the frequency and impact of any disruption to supply and so its primary benefit is to avoid the incidents that may otherwise disrupt supply and cause economic loss.

Economic impacts of disruptions to electricity supply

Damage to critical electricity assets can subsequently disrupt the generation, transmission and/or distribution of electricity to businesses and households. These events can generate costly immediate and longer-term impacts on the Australian economy. The immediate impacts of an electricity outage are those associated with loss of access to electricity or increased electricity costs, such as:

- Lost production (e.g. production of goods and services may cease);
- Lost productivity (e.g. workers may be idle whilst continuing to receive wages);
- Lost wages (e.g. workers may be sent home or unable to go to work);
- Spoiled goods (e.g. spoiled produce due to lack of refrigeration); and
- Increased cost of production if switching to a substitute source of energy (e.g. backup generator).

Quantifying the economic impacts associated with power outages is complex. Data is relatively sparse, and the economic impacts vary as they are highly sensitive to factors including:

- Duration of the power outage, for example short power outages are relatively manageable;
- Geographic spread of the outage, for example a localised power outage means that less users are affected and that substitutable goods (such as takeaway food) may be within travelling distance;
- Time of day/day of the week/time of the year that the outage occurs for example a power outage during business hours in the summer months will likely result in a larger economic impact than the same outage occurring in the middle of the night in winter; and
- The existence of any pre-established solutions to substitute electricity during the outage.

Computable General Equilibrium (CGE) modelling was used to illustrate how costly the disruption could potentially be by examining a hypothetical supply shock (i.e. less electricity is available to users) and an associated increase in input costs (i.e. an increase in the cost of electricity). The advantage of using a CGE approach is that both the direct and indirect (i.e. flow-on) economic impacts of a power outage event can be quantified.

CGE Modelling Approach

To analyse the direct and indirect economic contributions of power outages due to disruptions to critical infrastructure on the Australian economy, a CGE approach was used to model 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 power outages 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 outages and the rest of the economy in a framework that combines detailed historical data with fundamental economic theory.

Power outage scenarios

The CGE modelling provided estimates regarding how sensitive the Australian economy is to a shock to the electricity system. This analysis was undertaken by defining a set of hypothetical scenarios with varying magnitudes of power outages and price impacts associated with the power outage. The scope of the hypothetical scenarios was based on studies of major events which are discussed below.

Case studies

A series of case studies provides some context for how unplanned outages in the electricity network impact the economy. These case studies provide a basis for modelling hypothetical, but comparable outages, in an economy-wide (CGE) model and contextualising the results of that modelling. Case studies have been chosen to provide insights into the economy-wide costs to households and businesses of large-scale and severe power outages. The case studies include one domestic event, the 2016 South Australian blackout, and two international events, the 2003 US/Canada network failure and the 2003 Italian power outage. The table below provides a summary of the three case studies.

Power outage case studies in Australia and globally

Incident	Summary of incident
South Australian Blackout (2016)	On 28 September 2016, South Australia experienced a state-wide blackout. This was triggered by severe weather that damaged transmission and distribution assets, followed by reduced wind farm output and a loss of synchronism causing the loss of the Heywood Interconnector. The subsequent imbalance in supply and demand resulted in the remaining

	electricity generation in the state shutting down. While most supplies were restored in 8 hours, the wholesale market in South Australia was suspended for 13 days.[327]
US/Canada Network Failure (2003)	On 14 August 2003, large portions of the Midwest and Northeast US and Ontario, Canada, experienced an electric power blackout. The outage affected an area with an estimated 50 million people and 61,800 MW of electric load in Ohio, Michigan, Pennsylvania, New York, Vermont, Massachusetts, Connecticut, New Jersey and the Canadian province of Ontario. The power was not restored for 4 days in some parts of the US. Parts of Ontario suffered rolling blackouts for more than a week before full power was restored. Estimates of total costs in the US range between $4 billion and $10 billion (in US dollars). In Canada, gross domestic product was down 0.7% in August, there was a net loss of 18.9 million work hours, and manufacturing shipments in Ontario were down $2.3 billion (in Canadian dollars).[328]
Italian Power Outage (2003)	The 2003 Italy blackout, caused by a network failure, affected all of the Italian Peninsula for 12 hours and part of Switzerland near Geneva for 3 hours on 28 September 2003. It was the largest blackout in the series of blackouts in 2003, involving about 56 million people. Significant knock-on effects occurred across other critical infrastructures. Commercial and domestic users suffered disruption up to 48 hours. Cost to restaurants and bars in spoiled products and lost sales totalled up to about $139 million (in US dollars).[329]

While this RIS seeks to leverage the examples outlined above, it does not mean that a single, equivalent event is needed for costs and benefits to break even. The chosen examples are intended to be demonstrative of potential costs only, rather than the specific events which may lead to disruption. It may be the case that a series of smaller, less significant disruptions occur over the course of a year and accumulate to result in disruption of a similar scale.

The above case studies highlight that widespread power outages inflict substantial direct and indirect costs on firms and households alike. Businesses bore the brunt of the damage across all three case studies, mostly through lost income and productivity. It appears that manufacturing is hit particularly hard by blackouts; for instance, data from the Italian outage suggests that the manufacturing sector alone suffered 40% of total costs associated with the incident. Furthermore, the US/Canada network failure forced Daimler Chrysler to scrap around 10,000 cars moving through paint shops at time of outage. It also caused the solidification of molten metal inside a furnace at a Ford plant that took one week to repair. Severe industry-specific economic impacts, such as those experienced by Daimler Chrysler and Ford, are not identified by data-driven economic models – these impacts are revealed through observation of specific incidents.

For the purposes of the modelling of the cost of avoided future incidents in Australia, the South Australian blackout of 2016 was used as the baseline (moderate) risk scenario. The use of an actual event as the baseline risk point of comparison is important because it ensures the benefits analysis is grounded in reality. The scale of the event is not theoretical and there is sufficient information about the event to support modelling. The 2016 South Australian blackout was estimated to have approximately 5-8 GWh of unserved energy (electricity that would otherwise have been used by customers but that was not available because of the supply interruption).[330] Further, while an event of this magnitude has previously been considered to represent the worst-case power outage incident in Australia, the increasing severity and frequency of similar incidents detailed in section 1.1, particularly in the context of growing all hazards incidents, represents a risk to the whole economy.

A framework for considering the potential impacts of Australian power outages following failure of critical infrastructure is provided in the table below.

[327] Australian Energy Regulator, 2018.

[328] US – Canada Power Outage Task Force, 2004

[329] CRO Forum, 2011

[330] AEMO, 2018, Australian Energy Regulator, 2020; AEMC, 2019.

Framework for scenario development and sensitivity analysis

	Severe scenario	Moderate scenario	Low scenario
Intensity of event	150% of moderate scenario costs	South Australian 2016 Blackout	50% of moderate scenario costs

The rationale for a more severe scenario than experienced in South Australia reflects the complexity of the scenarios that could occur. As noted above, the economic impact of an incident will vary due to a range of factors including the location of a disruption, the month and time of day at which the disruption occurs, the day of the week on which the disruption takes place and the duration of disruption. Accounting for an incident that has a greater economic impact than the South Australian blackout is necessary to reflect the possibility that a disruption of the same scale (in terms of unserved energy) could impact areas where there would be greater economic impact than in South Australia in September at 4 pm. While an incident with a much greater impact than the severe scenario is conceivable (for example, a cyber-caused outage could be highly disruptive, by impacting a number of critical electricity assets in the grid simultaneously), the defined scenarios and subsequent benefits analysis has taken a deliberately conservative approach to ensure the severe scenario remains demonstrably plausible.

A summary of the economic impact of each scenario is provided in the table below. Direct avoided costs refer to the financial costs directly incurred as a result of an incident, while indirect costs refer to flow-on costs to the economy due to supply chain linkages and other feedback responses by all economic agents (e.g., households, businesses). A break-even analysis of these benefits compared to the total estimated cost of the risk management program framework is also included in the table. This break-even analysis is expressed as the number of incidents that would need to be avoided in order for the benefits (that is, the avoided costs) of the risk management program framework to equal the costs of implementation and compliance.

Summary of benefits scenarios

	Scenario 1 (Severe), $ million	Scenario 2 (Moderate), $ million	Scenario 3 (Low), $ million
Direct avoided cost	585.0	390.0	195.0
Indirect avoided costs	695.0	460.0	295.0
Total avoided cost to the economy of the incident	**1,280.0**	**850.0**	**490.0**
Approximate number of avoided incidents per annum required for a net benefit	0.5	0.7	1.2

Notes:

(a) According to Blackout Survey Results by Business South Australia (2016), total costs to South Australian businesses reached $390 million (inflated into 2020 Australian dollars) as a result of the power outage.

(b) In response to the 2016 blackout, the South Australian government installed a Tesla battery to improve their resilience to future events. As a result, indirect costs include the capital cost for installing the battery ($90 million) and costs for provision of network services ($4 million per year over 10 years).

As noted above, the total direct ongoing cost for option 2 is expected to be $228.0 million per annum plus direct one-off costs of $463.3 million. However, the cost of the risk management program framework would also have other indirect costs flowing from increased electricity prices passed onto consumers from the framework's implementation.

After considering the economy-wide impact of this change to the cost of providing electricity, the total economic cost of the regulatory changes, including direct and indirect costs would be approximately $595.4 million per year.[331] In order for the regulatory changes to generate a net benefit, the proposed risk management program framework would need to contribute to the prevention of approximately 1 low scenario incidents every year, 0.5 moderate scenario incidents every year or less than 1 severe scenario every two years to generate a net benefit.

It is important to note that the economic analysis of the above scenarios does not incorporate all direct avoided costs incurred by all future incidents. The avoided costs included are only those which were directly and immediately incurred as a result of the South Australian incident. In the broader context of a potential future disruption, in addition to the above estimate of benefits would be the avoided costs of recovery (repair costs, costs of resulting mitigations) from high value, specific circumstances which were not experienced during the South Australian blackout. For example, a disruption that shut down an Australian steel or aluminium manufacturer could cause significant repair costs or production loss for those entities in the same way that the Daimler Chrysler example noted above forced the scraping of around 10,000 cars. Consequently, the moderate case of a repeat South Australian incident is not likely to be the worst-case incident and an incident of the same scale in terms of electricity disruption could have a greater impact if it occurred in other locations.

Further, the increasing frequency of incidents as described in section 1.1 makes the proposed risk management program framework more certain over time to exceed the anticipated costs. The

[331] The total economic cost (being direct and indirect costs) was determined using the same CGE model approach used to estimate the benefits scenarios above. Total economic cost was determined by the CGE model and was based on an assumed economic shock equal to the cost of the draft risk management program framework (being a one-off cost of $463.3 million and an ongoing cost of $228.0 million). This resulted in a total economic impact of $595.4 million per year for the moderate scenario.

CGE modelling is a whole-of-economy approach that represents the Australian 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. In this context, indirect costs refer to flow-on costs to the economy due to supply chain linkages and other feedback responses by all economic agents (e.g. households, businesses), including those due to changes in prices or a decline in production caused by the absence of electricity supply.

examples referred to in that section demonstrate the increasing need for adequate protections against the security and resilience of critical electricity assets, and the increased likelihood that the benefits of the draft risk management program framework will exceed the costs outlined in this section.

Assessment of likely net benefit

The likely benefits of option 2 will be at least (and are expected to be more than) the costs of the regulation. This is primarily because, as described above and throughout this RIS, the frequency and severity of all hazard risks for critical electricity assets are growing. While some events of the magnitude described in this RIS 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, as described above, makes the proposed risk management program framework more likely to exceed the anticipated costs over time.

Further, through pursuit of option 2, the identification, mitigation and remediation of such hazards, should they occur, will be improved through:

- Lowering the material risk of hazards and subsequent impacts of those hazards, as they manifest for critical electricity assets;
- Ensuring that adoption of the risk management program framework for critical electricity assets is reasonable and proportionate to the purpose of the program;
- Avoiding regulatory duplication and facilitating a coordinated uplift in responsible entities' compliance with relevant standards; and
- Improving Government's visibility over the security and resilience of critical electricity assets.

Overall, these factors and the specific costs and benefits described above mean the likely net benefit associated with option 2 is high.

Appendix T: Detailed costing information for critical gas assets

Costing process completed by responsible entities for critical gas assets

Cost submissions were submitted by 12 responsible entities for critical gas assets. This represented approximately 20.0% of the total critical gas asset market.

The market share percentage of responsible entities who made a submission was calculated using entity and gas industry data sourced from IBISWorld.[332] [333] The market share of submissions was first determined at a business type level (gas supply, pipeline transport and gas extraction) by summing the business type market share percentage for individual entities. The market share of submissions at each individual business type level was then used to extrapolate the total critical gas assets market share represented by submissions.

To extrapolate the costs of compliance to all critical gas assets, organisations were categorised by size into 'large' and 'small' entities based on the following definitions:

- 'Large' entity - any entity with greater than 5% of critical gas assets' revenue in each business type (gas supply, pipeline transport and gas extraction).
- 'Small' entity - any entity with less than 5% of critical gas assets' revenue in each business type (gas supply, pipeline transport and gas extraction).

Critical gas asset cost impact submissions

Critical gas assets	Organisation size	Number of submissions
Critical gas asset entities	Large	6
	Small	6
Total		**12**

Likely net benefit – option 2

The following section details the costs and benefits associated with option 2 (the regulatory option), before assessing the overall likely net benefit presented by this option.

Costs of option 2

There are multiple factors affecting the regulatory burden for each entity, including their existing risk management practices and capabilities, the nature of the critical gas assets they operate and the size of their operations. In collecting cost information from entities across critical gas assets, this variance in cost impact has been captured and reflected in the estimates of total cost across critical gas assets included in this RIS.

When estimating the cost of compliance with option 2, critical gas asset entities provided both an expected and a high-cost estimate. The high-cost estimate was provided as a way to measure the uncertainty associated with their estimates and the highest feasible cost of option 2. The expected estimate was used as the basis for determining the net benefit of option 2 in section 4.

332 IBISWorld, 2021

333 Ibid

Using the expected and the high estimate as a range, the cost of compliance is as follows:

- A one-off regulatory cost of between $321.1 million (expected) and $945.3 million (high estimate), across critical gas assets nationally; and
- An ongoing cost of between $94.0 million (expected) and $219.2 million (high estimate) per year, across critical gas assets nationally.

The cost of regulation will be borne by entities responsible for critical gas assets who meet the relevant thresholds. Community organisations and individuals will not be directly affected but there will likely be indirect costs passed onto consumers. For the purposes of this RIS, the cost of regulation in the table below will only include the initial costs associated with regulation[334]. The indirect cost to consumers and communities has been addressed in the economic analysis through consideration of indirect cost to the wider economy as a result of the proposed risk management program framework.

Regulatory cost estimate

Cost Type	Costs ($ million)			
	Business	Community	Individuals	Total cost ($ million)
One-off	321.1 to 945.3	nil	nil	321.1 to 945.3
Ongoing (per year)	94.0 to 219.2	nil	nil	94.0 to 219.2

Note: There will be no direct costs to individuals and communities although price rises may reflect the increased cost of operations as a result of the proposed Risk Management Program framework.

The average cost of compliance for each entity is estimated at $10.5 million in one-off costs and $2.1 million per year in ongoing costs, noting that there is a wide range provided in submissions from industry. Entity costs range between $0.4 million and $55.9 million in one-off costs and $0.2 million and $5.0 million in ongoing costs per year. There are a number of reasons for this range in cost including the size of the entity and the maturity of existing risk management programs.

Based on the industry submissions made during consultations, the expected total regulatory costs will be highest for rules and obligations associated with addressing cyber and information security hazards. These costs represent approximately 29.1% of the total expected cost of implementing the risk management program framework. The cost associated with physical hazard rules (19.8% of total cost), supply chain hazard rules (17.6% of total cost) and personnel hazard rules (11.7% of total cost) are less significant but remain material. Compliance costs associated with material risk rules, risk management program rules, natural hazard rules and general rules were the least costly aspects of the risk management program framework, representing in total approximately 21.8% of costs in total. It is noted however, that the relative weightings of costs vary between entities based on their business types and operational environment. The total regulatory cost by rule/obligation is set out in the table below.

Regulatory burden estimate by rule and obligation for critical gas assets nationally

Rule / obligation	Costs (Expected and High)			
	One-off ($ million)	Ongoing (per year, $ million)	Total cost over 10 years ($ million) [335]	Expected estimate as percentage of

[334] Department of Prime Minister and Cabinet, 2020.

[335] For the purposes of calculating a total 10 year cost of compliance with the risk management program framework, ongoing costs were assumed to commence in the year after the required implementation date (for example, for a rule requiring implementation within 2 years, the ongoing costs associated with the rule were assumed to start in year 3 of the 10 year period).

				total (%)
Risk management program obligations in the Act	19.3 to 24.6	7.1 to 14.5	83.1 to 155.1	7.2
General rules	10.9 to 13.9	2.6 to 4.8	34.0 to 56.8	2.9
RMP rules				
Cyber and information security hazard	91.0 to 177.3	28.7 to 54.3	335.2 to 617.4	29.1
Personnel hazard	18.1 to 26.0	12.2 to 32.3	135.5 to 309.1	11.7
Supply chain hazard	56.4 to 480.3	16.3 to 35.1	203.5 to 795.9	17.6
Physical hazard	92.7 to 177.3	15.0 to 45.4	227.8 to 586.0	19.8
Natural hazard	10.3 to 19.0	3.9 to 7.1	45.6 to 82.6	4.0
Material risk	14.6 to 34.8	8.2 to 25.8	88.3 To 266.9	7.7
Total critical gas assets	**321.1 to 945.3**	**94.0 to 219.2**	**1,152.9 to 2,859.8**	**100.0**

Note: For the purposes of calculating a total 10-year cost of compliance with the risk management program framework, ongoing costs were assumed to commence in the year after the required implementation date (for example, for a rule requiring implementation within 2 years, the ongoing costs associated with the rule were assumed to start in year 3 of the 10 year period).

Following the design of sector specific rules and the submission of costs from Industry, the sector specific rules were updated to the sector agnostic Risk Management Program Rules. The Department confirmed with industry that no additional costings would be requested on the updated Risk Management Program rules, as they were either similar to the previously costed rules or a specific rule had been removed. For the purpose of the above estimate of regulatory burden, the original cost submissions provided by industry were used with the removed rules excluded.

The table below compares the share of regulatory cost for large industry participants (market share by revenue greater than 5%) and small industry participants (market share by revenue less than 5%) using the expected estimate. Large industry participants will incur approximately 57.0% of the total regulatory burden compared to 43.0% for small participants.

Distribution of expected regulatory cost compared to market share by entity size

Cost	**10-year costs (Expected)**			
	Large entities by market share		Small entities by market share	
	Cost ($ million)	Percentage of total costs (%)	Cost ($ million)	Percentage of total costs (%)
Total critical gas assets	657.3	57.0	495.6	43.0

The industry submissions also indicated the type of expenditure expected to be incurred. The allocation of cost between labour effort, capital and operating costs is provided in the table below.

The analysis of the expected estimates shows that 67.1% of one-off costs and 18.2% of ongoing costs are expected to be invested in capital. A relatively small share of costs are associated with labour effort (13.0% of one-off costs and 26.0% of ongoing costs) with operating costs being the largest component of ongoing costs (55.8% of total ongoing costs).

The allocation of ongoing costs reflects that significant costs are related to cyber-security hazards and this activity will require not only additional capital investment but also ongoing software and other service costs (e.g. because of the requirement for additional ongoing licenses and cloud services) in addition to labour effort.

Expected one-off and ongoing costs by cost type for critical gas assets nationally

Cost Type	Costs (Expected)			
	One-off ($ million)	One-off (%)	Ongoing (per year)	Ongoing (%)
Labour effort	41.7	13.0%	24.4	26.0%
Capital	215.4	67.1%	17.2	18.2%
Operating	64.1	19.9%	52.5	55.8%
Total critical gas assets	**321.1**	**100.0%**	**94.0**	**100.0%**

Benefits of option 2

A reliable continuous gas supply is central to Australia's prosperity. Further, disruption to supply can be a significant cost to the economy. The risk management program framework aims to reduce the frequency and impact of any disruption to supply and so its primary benefit is to avoid the incidents that may otherwise disrupt supply and cause economic loss.

Economic impacts of disruptions to gas supply

Disruption to the production, storage and distribution of gas will adversely impact the gas industry and its customers, businesses and households. Such disruptions can have costly immediate and longer-term impacts on the Australian economy. The immediate impacts of a gas outage are those associated with loss of access to gas or increased gas costs, such as:

- Lost production (e.g. production of goods and services may cease);
- Lost productivity (e.g. workers may be idle whilst continuing to receive wages);
- Lost wages (e.g. workers may be sent home or unable to go to work);
- Increased cost of production if switching to a substitute source of energy (e.g. backup generator).

Computable General Equilibrium (CGE) modelling was used to illustrate how costly gas disruptions could potentially be by examining a hypothetical supply shock (i.e. less gas is available to users) and an associated increase in input costs (i.e. an increase in the cost of gas). The advantage of using a CGE approach is that both the direct and indirect (i.e. flow-on) economic impacts of a gas outage event can be quantified.[336]

Modelling Approach

To analyse the direct and indirect economic impacts of unplanned outages in the gas network due to disruptions to critical infrastructure on the Australian economy, a CGE approach was used to model 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,

[336] Direct economic impacts refer to the 'first-round' effects that occur directly as a result of an incident, while indirect economic impacts refer to flow-on effects to the economy due to supply chain linkages and other feedback responses by all economic agents (e.g., households, businesses).

including consumers, investors, producers and governments operating in domestic and foreign goods, capital and labour markets.

The modelling framework is suited to analysing the economic impact of a gas supply disruption 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 gas disruption incident and the rest of the economy in a framework that combines detailed historical data with fundamental economic theory.

Scenarios

The CGE modelling provided estimates regarding how sensitive the Australian economy is to a shock to the gas system. This analysis was undertaken by deriving a set of hypothetical modelling scenarios based on assumptions about the intensity of a gas outage, with the initial impact calibrated as reduction in the quantity of gas supplied and the normalised insurance costs as a result of an event. The hypothetical scenarios were informed by studies of major events, which are discussed below.

Case studies

The case studies provided in the table below provide a basis for modelling hypothetical, but comparable outages, in an economy-wide model and contextualising the results of that modelling. Case studies have been chosen to provide insights into the economy-wide costs to households and businesses of large-scale and severe gas disruption events. The case studies include three domestic events in Western Australia and Victoria (Varanus Island disruption in 2008, Longford plant explosion in 1998 and Longford disruption in 2021), and two international events (the 2018 Enbridge pipeline explosion in Canada and the 2020 natural gas compressor cyber-attack in the US).

Incident	Summary of incident
Domestic incidents	
Varanus Island disruption, Western Australia (2008)	In June 2008, a major disruption to the natural gas supply in Western Australia occurred due to the rupture of a corroded pipeline and the subsequent explosion at a processing plant on Varanus Island, off the state's north west coast. The Apache Energy's plant was shut down, reducing Western Australia's gas supply by around 30% for over two months. Gas spot prices increased sharply, and several mining and industrial companies were forced to curtail production. Some electricity generators switched to emergency diesel stocks, and coal fired power plants that had been closed were also brought back online.[337]
Longford plant explosion, Victoria, Australia (1998)	The explosion at the Longford Esso/BHP gas processing facility near Sale, Victoria in September 1998 severely disrupted the entire Victorian gas supply and left Victorians without gas supplies for 10 days[338]. There were several factors which led to the explosion, these included a lack of adequate training for staff, lack of comprehensive operating procedures and insufficient technical support on site. The plant was shut down immediately following the explosion and Victoria was left without its primary gas supplier. Within days, the Victorian Energy Networks Corporation shut down the state's entire gas supply. Reports have suggested the disruption cost Victorian businesses about $1.3 billion.[339]
Longford disruption,	The Longford gas plant in Victoria, the largest domestic gas production plant on the east coast suffered another disruption to production over a weekend in mid-July 2021, triggering

[337] Government of Western Australia – Office of Energy, *Gas Supply and Emergency Management Committee – Report to Government,* September 2009.

[338] Australian Broadcasting Corporation, *Longford gas plant workers remembered 20 years on from deadly explosion,* September 2018

[339] Parliament of Australia, *Natural gas: energy for the new millennium,* December 1998.

Victoria, Australia (2021)	a spike in prices. Victorian wholesale gas price jumped to $39.99 a gigajoule on Saturday afternoon, about six times the average earlier in the year. The plant's production was reduced by about 30-35% for more than 24 hours due to technical problems.[340]
Overseas incidents	
Enbridge pipeline explosion, Canada (2018)	In 2018, undetected stress corrosion cracking saw the rupture of Canada's Enbridge natural gas pipeline, resulting in a fire near the city of Prince George in the province of British Columbia. The rupture forced the evacuation of approximately 125 residents within a 2km radius of the explosion site, resulted in province-wide natural gas shortages and required heightened energy conservation efforts throughout winter. About 10% of Western Canada's gas supply was lost for two days, and operations were restricted for a total of 21 days.[341]
US natural gas compressor cyber-attack (2020)	A major US natural gas compression facility was entirely shut down for two days due to a ransomware attack, causing loss of productivity and revenue, according to a security alert issued by the US Cybersecurity and Infrastructure Security Agency (CISA). The attacker deployed the commodity ransomware to encrypt data on both the operational and information technology networks at the same time before demanding a ransom payment.[342]

These case studies highlight that gas outages inflict substantial direct and indirect costs on firms and households alike. Businesses bore the brunt of the damage across all case studies, mostly through lost income and productivity. It appears that both industrial and commercial sectors (particularly, the hospitality industry, which used natural gas as an intermediate input for cooking and space heating) are hit hard by gas supply shortages. For instance, studies into the Longford plant explosion in 1998 disruption found the loss to industry during the crisis was estimated at about $1.3 billion, with Victorian industries that had lost their energy source being forced to close. During the Longford disruption in 2021, manufacturers that were exposed to the spot market were hurt by the spiking gas prices. The Enbridge pipeline explosion in Canada in 2018 resulted in a gas supply deficit the in the FortisBC system, forcing supply to hospitals, refineries, food and other processing facilities, and condominium complexes to be cut off entirely. Residents are also likely to experience a high degree of inconvenience due to gas shortages, impacting hot water or heating.

For the purposes of the modelling of the cost of avoided future incidents in Australia, the Varanus Island disruption was selected to be simulated due to the availability of sufficient information about its direct impact on gas supply to support the modelling. Given the major magnitude of damages, this incident is considered a severe risk scenario. The use of an actual event as a risk point of comparison is important because it ensures the benefits analysis is grounded in reality. The plant, which normally supplied a third of the state's gas, was closed for almost two months. Supply from the plant partially resumed in late August. By mid-October, gas production was running at two-thirds of normal capacity with 85% of fully capacity restored by December 2008. It is estimated that approximately 40-50 petajoules, or 4-5% of total national gas supply, was lost in 2008.[343] According to the Insurance Council of Australia, the normalised insurance losses were about $279 million (in 2011 dollars) or $340 million (in 2021 dollars).[344] The estimate of insurance losses should be interpreted with caution – a senate inquiry into matters relating to the explosion indicated that the relatively modest insurance impact reflected most companies choosing not to take out business disruption insurance, and in several cases, policies only allowing a claim if gas supply was completely cut off rather than just being reduced or subject to high deductibles.[345]

[340] Australian Financial Review, *Longford disruption ups pressure on east coast gas as prices spike,* July 20.

[341] Transportation Safety Board of Canada, *Pipeline Transportation Safety Investigation Report,* October 2018.

[342] US Cybersecurity and Infrastructure Security Agency, *Alert – Ransomware impacting pipeline operations,* October 2020.

[343] This is estimated using the timeline of the Varanus Island event and information about the quantity of gas demand and production sourced from the State of the Energy Market 2008 by Australian Energy Regulator.

[344] Australian Institute for Disaster Resilience, *Varanus Island gas explosion 2008*, June 2008.

[345] The Senate Standing Committee on Economics, *Matters relating to the gas explosion at Varanus Island, Western Australia,* December 2008.

A framework for considering the potential impacts of Australian gas outages following failure of critical infrastructure is provided in the table below.

Framework for scenario development and sensitivity analysis

	Severe scenario	Moderate scenario	Low scenario
Intensity of event	Varanus Island disruption in 2008[346]	50% of severe scenario gas supply loss	25% of severe scenario gas supply loss

The rationale for a more severe scenario than experienced in the Varanus Island incident reflects the complexity of the scenarios that could occur. As noted above, the economic impact of an incident will vary due to a range of factors including the location of a disruption, as well as the timing and the duration of disruption. While an incident with a much greater impact than the severe scenario is conceivable, the defined scenarios and subsequent benefits analysis are based on a deliberately conservative approach to ensure the severe scenario remains demonstrably plausible.

A summary of the economic impact of each scenario is provided in the table below. A break-even analysis of these benefits compared to the total estimated cost of the risk management program framework is also included in the table. This break-even analysis is expressed as the number of incidents that would need to be avoided in order for the benefits (that is, the avoided costs) of the risk management program framework to equal the costs of implementation and compliance.

Summary of benefits scenarios

	Scenario 1 (Severe), $ million	Scenario 2 (Moderate), $ million	Scenario 3 (Low), $ million
Total avoided cost to the economy of the incident	**1,913.0**	**1,001.0**	**513.0**
Approximate number of avoided incidents per annum required for a net benefit	0.1	0.2	0.3

As noted above in the cost of option 2, the total direct ongoing cost for option 2 is expected to be $94.0 million per annum plus direct one-off costs of $321.1 million. However, the cost of the risk management program framework would also have other indirect costs flowing from increased gas prices passed onto consumers from the framework's implementation.

After considering the economy-wide impact of this change to the cost of providing gas, the total economic cost of the regulatory changes, including direct and indirect costs would be approximately $159.0 million per year.[347] In order for the regulatory changes to generate a net benefit, the proposed risk management program framework would need to contribute to the

[346] Total avoided cost of the incident to the economy is based on a conservative economy-wide impact estimation of an incident that results in a 4-5% gas supply shortage in annual terms to the national economy and the estimated normalised insurance cost of about $340 million (in 2021 dollars).

[347] The total economic cost (being direct and indirect costs) was determined using the same CGE model approach used to estimate the benefits scenarios above. Total economic cost was determined by the CGE model and was based on an assumed economic shock equal to the cost of the draft risk management program framework (being a one-off cost of $321.1 million and an ongoing cost of $94.0 million). This resulted in a total economic impact of $159.0 million per year for the moderate scenario.

CGE modelling is a whole-of-economy approach that represents the Australian 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. In this context, indirect costs refer to flow-on costs to the economy due to supply chain linkages and other feedback responses by all economic agents (e.g. households, businesses), including those due to changes in prices or a decline in production caused by the absence of gas supply.

prevention of approximately 1 low scenario incident approximately every 3 years, approximately 1 moderate scenario incident every 6 years or approximately 1 severe scenario every 12 years to generate a net benefit.

It is important to note that the economic analysis of the above scenarios may not incorporate all direct avoided costs incurred by all future incidents. In the broader context of a potential future disruption, in addition to the above estimate of benefits would be the avoided costs of recovery (repair costs, costs of resulting mitigations, productivity loss due to attending to legal ramifications, intangible costs on the environment, health and wellbeing, loss of reputation etc.) from high value, specific circumstances which were not experienced during the Varanus Island event. For example, the Enbridge incident in Canada forced 125 residents within a 2km radius of the explosion site to evacuate, and the Longford incident in 1998 caused two deaths and eight injuries.

Further, the increasing frequency of incidents as described in section 1.1 makes the proposed risk management program framework more certain over time to exceed the anticipated costs. The examples referred to in that section demonstrate the increasing need for adequate protections against the security and resilience of critical gas assets, and the increased likelihood that the benefits of the draft risk management program framework will exceed the costs outlined in this section.

Assessment of likely net benefit

The likely benefits of option 2 will be at least (and are expected to be more than) the costs of the regulation. This is primarily because, as described above and throughout this RIS, the frequency and severity of all hazard risks for critical gas assets are growing. While some events of the magnitude described in this RIS 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, as described above, makes the proposed risk management program framework more likely to exceed the anticipated costs over time.

Further, through pursuit of option 2, the identification, mitigation and remediation of such hazards, should they occur, will be improved through:

- Lowering the material risk of hazards and subsequent impacts of those hazards, as they manifest for critical gas assets;
- Ensuring that adoption of the risk management program framework for critical gas assets is reasonable and proportionate to the purpose of the program;
- Avoiding regulatory duplication and facilitating a coordinated uplift in responsible entities' compliance with relevant standards; and
- Improving Government's visibility over the security and resilience of critical gas assets.

Overall, these factors and the specific costs and benefits described above mean the likely net benefit associated with option 2 is high.

Appendix U: Detailed costing information for critical water assets

Costing process completed by responsible entities for critical water assets

Cost submissions were received from 7 responsible entities for critical water assets. This represented approximately 33.3% of the total critical water and sewerage asset market.

The market share percentage of responsible entities who made a submission was calculated using entity and water and sewerage business type (water supply, sewerage services and water treatment services) data sourced from IBISWorld. The market share of submissions was first determined at the water and sewerage business type level by summing the entity market share percentages. The total market share of submissions at each individual business type level was then used to extrapolate the total critical water assets market share represented by submissions.

To extrapolate the cost of compliance to all critical water assets, organisations were categorised by size into 'large' and 'small' entities based on the following definitions:

- 'Large' entity - any entity with greater than 5% of critical water assets' revenue in each business type (water supply, sewerage services and water treatment services).
- 'Small' entity - any entity with less than 5% of critical water assets' revenue in each business type (water supply, sewerage services and water treatment services).

Critical water asset cost impact submissions

	Organisation size	Number of submissions
Critical water assets	Small	4
	Large	3
Total		**7**

Likely net benefit – option 2

The following section details the costs and benefits associated with option 2 (the regulatory option), before assessing the overall likely net benefit presented by this option.

Costs of option 2

There are multiple factors affecting the regulatory burden for each entity, including their existing risk management practices and capabilities, the nature of the critical water assets they operate and the size of their operations. In collecting cost information from entities across critical water assets, this variance in cost impact has been captured and reflected in the estimates of total cost across critical water assets included in this RIS.

When estimating the cost of compliance with option 2, critical water and sewerage asset entities provided both an expected and a high-cost estimate. The high-cost estimate was provided as a way to measure the uncertainty associated with their estimates and the highest feasible cost of option 2. The expected estimate was used as the basis for determining the net benefit of option 2 in section 4.

Using the expected and the high estimate as a range, the cost of compliance is as follows:

- A one-off regulatory cost of between $157.5 (expected) and $262.4 million (high estimate), across critical water assets nationally; and
- An ongoing cost of between $91.1 (expected) and $211.0 million (high estimate) per year, across critical water assets nationally.

The cost of regulation will be borne by entities responsible for critical water assets who meet the relevant thresholds. Community organisations and individuals will not be directly affected but there will likely be indirect costs passed onto consumers. For the purposes of this RIS, the cost of regulation in the table below will only include the initial costs associated with regulation.[348] The indirect cost to consumers and communities has been addressed in the economic analysis through consideration of indirect cost to the wider economy as a result of the proposed RMP framework.

The average cost of compliance for each entity is estimated at $14.4 million in one-off costs and $6.1 million per year in ongoing costs, noting that there is a wide range provided in submissions from industry. Entity costs range between $0.0 million and $60.1 million in one-off costs and $0.5 million and $19.2 million in on-going costs per year. There are a number of reasons for this range in cost including the size of the entity and the maturity of existing RMPs.

Regulatory cost estimate

Cost Type	Costs ($ million)			
	Business	Community	Individuals	Total cost
One-off	157.5 to 262.4	Nil	Nil	157.5 to 262.4
Ongoing (per year)	91.1 to 211.0	Nil	Nil	91.1 to 211.0

Note: There will be no direct costs to individuals and communities although price rises may reflect the increased cost of operations as a result of the proposed RMP framework.

Based on the industry submissions made during consultations, the expected total regulatory costs will be highest for rules and obligations associated with addressing physical and natural hazards. These costs represent approximately 52.9% of the total cost of implementing the RMP framework. The cost associated with cyber and information security hazards (35.6% of total cost) is lower but remains significant. Compliance costs associated with RMP obligations in the Act, general rules, personnel hazards, supply chain hazards and material risk rules were the least costly aspects of the RMP framework, representing in total approximately 11.5% of costs in total. The total regulatory cost by rule/obligation is set out in the table below.

Regulatory burden estimate by rule and obligation for critical water assets nationally

Rule / obligation	Costs (Expected and High)			
	One-off ($ million)	Ongoing (per year, $ million)	Total cost over 10 years ($ million) [349]	Expected estimate as percentage of total (%)
RMP obligations in the Act	2.4 to 4.5	3.1 to 4.5	30.0 to 44.7	3.0
General rules	1.6 to 3.2	0.2 to 0.2	3.3 to 5.2	0.3
RMP rules				

[348] Department of Prime Minister and Cabinet, 2020.

[349] For the purposes of calculating a total 10 year cost of compliance with the RMP framework, ongoing costs were assumed to commence in the year after the required implementation date (for example, for a rule requiring implementation within 2 years, the ongoing costs associated with the rule were assumed to start in year 3 of the 10 year period).

Cyber and information security hazard	35.4 to 82.7	35.5 to 48.1	358.2 to 434.1	35.6
Personnel hazard	4.0 to 5.0	3.2 to 4.3	34.4 to 44.1	3.4
Supply chain hazard	5.0 to 9.1	4.2 to 14.3	44.8 to 137.9	4.4
Physical and natural hazard	108.4 to 156.4	44.7 to 139.3	532.8 to 1,409.8	52.9
Material risk	0.8 to 1.4	0.3 to 0.4	3.5 to 5.0	0.3
Total critical water assets	**157.5 to 262.4**	**91.1 to 211.1**	**1,006.9 to 2,080.8**	**100**

The table below compares the share of regulatory cost for large industry participants (market share by revenue greater than 5%) and small industry participants (market share by revenue less than 5%). Large industry participants will incur approximately 50.1% of the expected total regulatory burden compared to 49.9% for small participants.

Distribution of expected regulatory cost compared to market share by entity size

Cost	10-year costs (Expected)			
	Large entities by market share		Small entities by market share	
	Cost ($ million)	Percentage of total costs (%)	Cost ($ million)	Percentage of total costs (%)
Total critical water assets	504.9	50.1	502.1	49.9

The industry submissions also indicated the type of expenditure expected to be incurred. The allocation of cost between labour effort, capital and operating costs is provided in the table below.

The analysis shows that 66.0% of one-off costs and 32.8% of ongoing costs are expected to be invested in capital. A relatively small share of costs are associated with labour effort (13.4% of one-off costs and 22.8% of ongoing costs) with operating costs being the largest component of ongoing costs (44.4% of total ongoing costs).

The allocation of ongoing costs reflects that significant costs are related to cyber and information security hazards and this activity will require not only additional capital investment but also ongoing software and other service costs (e.g. because of the requirement for additional ongoing licenses and cloud services) in addition to labour effort.

Expected one-off and ongoing costs by cost type for critical water assets nationally

Cost Type	Costs			
	One-off ($ million)	One-off (%)	Ongoing (per year)	Ongoing (%)
Labour effort	21.0	13.4	21.0	22.8
Capital	104.0	66.0	29.9	32.8
Operating	32.5	20.6	40.5	44.4

Total critical water assets	**157.5**	**100.0**	**91.1**	**100.0**

Benefits of option 2

A reliable continuous water and sewerage supply is central to Australia's prosperity. Further, disruption to supply can be a significant cost to the economy. The RMP framework aims to reduce the frequency and impact of any disruption to supply and so its primary benefit is to avoid the incidents that may otherwise disrupt supply and cause economic loss.

Economic impacts of disruptions to water and sewerage supply

Damage to critical water assets can disrupt the supply of water and sewerage to businesses and households. These events can generate costly immediate and longer-term impacts on the Australian economy. Globally, it is estimated that about 42% of the world's total active workforce is working in heavily water-dependent industries, where water is a necessary part of the sector's value chain.[350] The immediate impacts of a disruption to water and sewerage supply include:

- Slowed or lost production (e.g. where production is water-dependent);
- Reduced or lost productivity (e.g. workers may be idle whilst continuing to receive wages);
- Lost wages (e.g. workers may be sent home or unable to go to work);
- Increased cost of production if necessary alternatives to regular supply are required (e.g. water delivery).

In addition to the economic impacts, there are also qualitative impacts resulting from loss of access or compromise of a critical infrastructure asset that cannot be quantified using an economic method. This is true across all critical infrastructure sectors, however, is especially relevant in the context of critical water assets. Water is fundamental to life itself – the potential consequences of a loss of access to, or compromise of, a critical water asset go far beyond the financial burden that is placed upon a relevant entity or the broader economy. The United Nations General Assembly explicitly recognised the human right to water and sanitation through Resolution 64/292 – acknowledging that clean drinking water and sanitation are essential to the realisation of all human rights.

These potential consequences of a prolonged disruption to a critical water asset are discussed above in Appendix I, two key points include:

- A lack of safe and clean drinking water heightens risk of illness, disease, and ultimately threatens human life; and
- Lack of access to water and sanitation burden health systems, unable to meet cleanliness and safety standards.

Quantifying the economic impacts associated with a disruption to water supply is complex. Data is relatively sparse, and the economic impacts vary as they are highly sensitive to factors including:

- Duration of the disruption, for example short disruptions are relatively manageable;
- Geographic spread of the outage, for example a localised disruption to supply means that less users are affected and substitutable goods are available; and

[350] WWAP 2016

- Time of day/day of the week/time of the year that the outage occurs for example a water supply disruption during business hours in the summer months will likely result in a larger economic impact than the same outage occurring in the middle of the night in winter.

Noting these challenges, an approach to model the cost of a specific cyber incident on a water business was taken instead of quantifying the potential costs associated with a lack of water supply.

Computable General Equilibrium (CGE) modelling was used to illustrate how costly the incident could potentially be by examining the real-world cost of a data breach on a business in the water sector and an associated increase in input costs (i.e. an increase in the cost of water and sewerage). The advantage of using a CGE approach to determine quantitative benefit is that both the direct and indirect (i.e. flow-on) economic impacts of an incident can be quantified.

CGE Modelling Approach

To analyse the direct and indirect economic contributions of an incident on a critical water asset in the Australian economy, a CGE approach was used to model 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 an incident on a critical water asset 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 data breach scenario and the rest of the economy in a framework that combines detailed historical data with fundamental economic theory.

Scenario

The CGE modelling provided estimates regarding how sensitive the Australian economy is to a shock as a result of an incident in the water sector. This analysis is undertaken by defining a set of hypothetical scenarios with varying magnitude of impact and resulting cost. The scope of the hypothetical scenarios is based on real-world case studies. Discussed below are the case studies which informed the scope of the hypothetical scenario.

Case studies

The case studies provided in the table below provide a basis for modelling hypothetical, but comparable incidents, in an economy-wide model and contextualising the results of that modelling. Case studies have been chosen to provide insights into the economy-wide costs to households and businesses of disruption events. Available real-world case studies that can be applied to the Australian context are limited. As highlighted above, an approach that modelled the cost of a cyber incident was taken due to challenges associated with modelling the cost of a disruption to water supply.

Incident case studies affecting water assets in Australia and globally

Incident	Summary of incident
UK water supplier scam (2017)	Published in the 2017 Verizon Data Breach Digest Report, a UK water supplier discovered that bank account details of clients had been changed and a total of £500,000 (approximately AUD$812,000 in 2017) had been requested and sent to two bank accounts in England. The source of the breach was determined to be an employee working in the call centre to which the water supplier had outsourced its customer support operations.
Kemuri Water Company (2016)	In 2016, a company generically identified as Kemuri Water Company noticed that its water treatment centre was operating erratically, with chemical values being modified without any manual intervention from company employees. It was discovered that hackers proceeded to modify chemical parameters of the water treatment plant at random. Secondary systems discovered the sabotage in time to avoid a severe situation.
Sydney Water Crisis (1998)	Between July and September 1998, microscopic pathogens were detected in the water supply of Greater Metropolitan Sydney. The contamination was detected following routine water sampling and testing over a series of weeks. The crisis caused a mixture of fear, cynicism and anger in the community. The cost to Sydney Water was estimated to be $33 million (including lost revenue, rebates paid to customers, and damages claims). These costs do not include capital expenditures on improvements to the system and infrastructure following the incident.
Queensland floods (2010-2011)	A series of flooding events affected Queensland between November 2010 and February 2011, with catastrophic impacts across the state. The floods occurred in the wake of heavy rainfall caused by compounding extreme weather events. The impact to the state's economy was significant, with over $4 billion paid out in insurance claims and various relief payments. 33 lives were lost attributed to the floods, with a further three people missing.

For the purposes of the modelling of the cost of avoided future incidents in Australia, three baseline scenarios were identified, described above. Three baseline scenarios were selected to demonstrate the range of potential consequence as a result of a disruption to a critical water asset, with the scale of potential cost to the economy ranging from minimal to catastrophic.

The UK water supplier scam example was selected as the low baseline scenario. The incident was relatively limited in enduring impact, scale and duration, with the relatively minor cost to the organisation unlikely to have a significant impact on the economy or customers of the affected business.

The Sydney water crisis of 1998 was selected as the moderate risk scenario. The incident demonstrates the potential extent of disruption which can be caused as a result of water quality issues. Water contamination can result in severe economic and health consequences and individuals, and in this instance, there were a range of costs associated with determining the cause of contamination and a plan for rectification. While the cause of the incident was not a specific threat that this proposed regulatory framework will contribute to avoiding, threats to water quality that could have similar consequences have been documented, including in the case of the Kemuri Water Company case study discussed above. While in that instance the malicious activity was detected and the threat mitigated, it is reasonable to assume that the type of costs could be similar to what was experienced in the Sydney Water Crisis scenario (extensive testing to determine extent of contamination, potential rebates paid to customers, and damages claims) should this mitigation not have occurred. Costs were estimated to be $33.0 million in 1998 dollars. Adjusting for inflation the dollar-adjusted amount is $58.6 million. This figure is treated as the direct cost of the moderate risk scenario.

The Queensland floods of 2010 and 2011 was selected as the severe risk scenario. The floods were catastrophic in terms of consequences to individuals, business and the state as a whole. While this scenario did not occur as a result of the realisation of a specific hazard or threat (and was caused by compounding weather events) it demonstrates the potentially severe and widespread consequences of a disruption to a critical water asset (including the release of water from a dam) which could possibly be caused by a deliberate attack or incident. Insurance claims and relief payments as a result of the floods totalled $4.1 billion, while estimates of the total impact

to Australia's GDP reached $30 billion. Considering the aggregated nature of the payments reported, and consistent with the deliberately conservative approach to benefits analysis described above and throughout this RIS, the $4.1 billion figure is used as the total cost to the economy of the scenario.

The use of actual events as risk points of comparison is important because it ensures the benefits analysis is grounded in reality. A framework for considering the potential impact of incidents in the Australian water is provided in the table below.

Framework for scenario development and sensitivity analysis

	Severe scenario	Moderate scenario	Low scenario
Intensity of event	Queensland floods (2010-11)	Sydney water crisis (1998)	UK water supplier scam (2017)

As stated above, the water and sewerage sector is complex and diverse, and critical water assets range broadly in size, importance, number of customers serviced, and number of customers potentially affected in the case of compromise. The three scenarios described above provide real-world points of comparison to understand the potential range of consequences as a result of a disruption to critical water assets.

A summary of the economic impact of each scenario is provided in the table below. A break-even analysis of these benefits compared to the total estimated cost of the risk management program framework is also included in the table. This break-even analysis is expressed as the number of incidents that would need to be avoided in order for the benefits (that is, the avoided costs) of the risk management program framework to equal the costs of implementation and compliance.

Summary of benefits scenarios

	Scenario 1 (Severe), $ million	Scenario 2 (Moderate), $ million	Scenario 3 (Low), $ million
Direct avoided costs	4,099.0	58.6	0.7
Indirect avoided costs	-	68.2	0.5
Total avoided cost to the economy of the incident	4,099.0	126.8	1.2
Approximate number of avoided incidents per annum required for a net benefit	Less than 0.1	1.8	197.5

As noted above in the cost of option 2, the total direct ongoing cost for option 2 is expected to be $91.1 million per annum plus direct one-off costs of $157.5 million. However, the cost of the risk management program framework would also have other indirect costs flowing from increased water prices passed onto consumers from the framework's implementation.

After considering the economy-wide impact of this change to the cost of providing water, the total economic cost of the regulatory changes, including direct and indirect costs would be approximately $227.1million per year.[351] In order for the regulatory changes to generate a net

[351]The total economic cost (being direct and indirect costs) was determined using the same CGE model approach used to estimate the benefits scenarios above. Total economic cost was determined by the CGE model and was based on an assumed economic shock equal to the cost of the draft risk management program framework (being a one-off cost of $157.5 million and an ongoing cost of $91.1 million). This resulted in a total economic impact of $227.1 million per year for the moderate scenario.

benefit, the proposed risk management program framework would need to contribute to the prevention of approximately 195 low scenario incidents every year, approximately 1.8 moderate scenario incidents every year or one severe scenario every 18 years to generate a net benefit.

It is important to note that the economic analysis of the above scenarios may not incorporate all direct avoided costs incurred by all future incidents. In the broader context of a potential future disruption, in addition to the above estimate of benefits would be the avoided costs of recovery (repair costs, costs of resulting mitigations, productivity loss due to attending to legal ramifications, intangible costs on the environment, health and wellbeing, loss of reputation etc.).

Further, the increasing frequency of incidents as described in section 1.1 makes the proposed risk management program framework more certain over time to exceed the anticipated costs. The examples referred to in that section demonstrate the increasing need for adequate protections against the security and resilience of critical water assets, and the increased likelihood that the benefits of the draft risk management program framework will exceed the costs outlined in this section.

Assessment of likely net benefit

There are a range of economic factors to consider when assessing the likely net benefit of this regulation for critical water assets, demonstrated by the range of potential consequences as a result of compromise or disruption. Potential impacts of disruption range from catastrophic to relatively minor, with the frequency of incidents required to be avoided to generate a net benefit varying significantly.

As an additional complexity, the potentially significant economic consequences of a disruption to critical water assets could be insignificant in comparison to the potential consequences for human life because of reduced or limited access to water and sewerage, or indeed as a result of an event itself. As described above, limited, or reduced access to water can have grave consequences for a range of water-dependent critical services, such as hospitals or sanitation facilities, which in turn can lead to heightened risk of disease, illness or death. The estimated value of a statistical life (the value society places on reducing the risk of dying) is $5.1 million, and the value of a statistical life year (the value society places on a year of life) is $222,000.[352] As water is critical to human life, any avoidance of a disruption to critical water assets that could have otherwise increased the likelihood of disease, illness or death will have a benefit beyond that of the avoided cost to the economy able to be modelled.

The likely benefits of option 2 will be at least (and are expected to be more than) the costs of the regulation. This is because, as described above and throughout this RIS, the frequency and severity of all hazard risks for critical water assets are growing. While some events of the magnitude described in this RIS 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, as described above, makes the proposed risk management program framework more likely to exceed the anticipated costs over time. In addition, the potential risk to human life (through illness, disease or death) is heightened in this asset class due to the criticality of water to human life itself and the water-dependency of key critical services.

CGE modelling is a whole-of-economy approach that represents the Australian 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. In this context, indirect costs refer to flow-on costs to the economy due to supply chain linkages and other feedback responses by all economic agents (e.g. households, businesses), including those due to changes in prices or a decline in production caused by the absence of gas supply.

[352] Abelson 2007

Further, through pursuit of option 2, the identification, mitigation and remediation of such hazards, should they occur, will be improved through:

- Lowering the material risk of hazards and subsequent impacts of those hazards, as they manifest for critical water assets;
- Ensuring that adoption of the risk management program framework for critical water assets is reasonable and proportionate to the purpose of the program;
- Avoiding regulatory duplication and facilitating a coordinated uplift in responsible entities' compliance with relevant standards; and
- Improving Government's visibility over the security and resilience of critical water assets.

These factors and the specific costs and benefits described above mean the likely net benefit associated with option 2 is high.

Appendix T: Detailed costing information for critical data storage or processing assets

Costing process completed by responsible entities for critical data storage or processing assets

Six responsible entities for critical data processing or storage assets submitted an estimated cost of compliance for their entity.

Likely net benefit – option 2

The following section details the costs and benefits associated with option 2 (the regulatory option), before assessing the overall likely net benefit presented by this option.

Costs of option 2

There are multiple factors affecting the regulatory burden for each entity, including their existing risk management practices and capabilities, the nature of the critical data storage or processing assets they operate and the size of their operations. In collecting cost information from entities across critical data storage or processing assets, this variance in cost impact has been captured and reflected in the estimates of total cost across critical data storage or processing assets included in this RIS.

When estimating the cost of compliance with option 2, critical data storage or processing asset entities provided both an expected and a high-cost estimate. The high-cost estimate was provided as a way to measure the uncertainty associated with their estimates and the highest feasible cost of option 2. The expected estimate was used as the basis for determining the net benefit of option 2 in section 4.

Using the expected and the high estimate as a range, the cost of compliance is as follows:

- A one-off regulatory cost of between $116.6 (expected) and $150.1 million (high estimate), across critical data storage or processing assets nationally; and
- An ongoing cost of between $296.9 (expected) and $402.3 million (high estimate) per year, across critical data storage or processing assets nationally.

The cost of regulation will be borne by entities responsible for critical data storage or processing assets who meet the relevant thresholds. Community organisations and individuals will not be directly affected but there will likely be indirect costs passed onto consumers. For the purposes of this RIS, the cost of regulation in the table below will only include the initial costs associated with regulation[353]. The indirect cost to consumers and communities has been addressed in the economic analysis through consideration of indirect cost to the wider economy as a result of the proposed RMP framework.

The average cost of compliance for each entity is estimated at $1.7 million in one-off costs and $1.9 million per year in ongoing costs, noting that there is a wide range provided in submissions from industry. Entity costs range between $0.1 million and $8.5 million in one-off costs and $0.1 million and $8.0 million in on-going costs per year. There are a number of reasons for this range in cost including the size of the entity and the maturity of existing RMPs.

[353] Department of Prime Minister and Cabinet, 2020.

Regulatory cost estimate

Cost Type	Costs ($ million)			
	Business	Community	Individuals	Total cost
One-off	116.6 to 150.1	Nil	Nil	116.6 to 150.1
Ongoing (per year)	296.9 to 402.3	Nil	Nil	296.9 to 402.3

Note: There will be no direct costs to individuals and communities although price rises may reflect the increased cost of operations as a result of the proposed RMP framework.

Based on the industry submissions made during consultations, total regulatory costs will be highest for rules and obligations associated with addressing physical and natural hazards. These costs represent approximately 56.3% of the total cost of implementing the RMP framework. The cost associated with cyber and information security hazards (13.7% of total cost) is less significant but remains material. Compliance costs associated with RMP obligations, general rules, personnel hazards, supply chain hazards and material risk rules were the least costly aspects of the RMP framework, representing approximately 30.0% of costs in total. The total regulatory cost by rule/obligation is set out in the table below.

Regulatory burden estimate by rule and obligation for critical data processing or storage assets nationally

Rule / obligation	Costs			
	One-off ($ million)	Ongoing (per year, $ million)	Total cost over 10 years ($ million) [354]	Expected estimate as percentage of total (%)
RMP obligations in the SLACIP Act	8.4 to 12.8	34.6 to 53.4	319.6 to 493.2	11.0%
General rules	9.8 to 18.0	18.9 to 32.2	179.9 to 307.4	6.2%
RMP rules				
Cyber and information security hazard	30.7 to 40.3	39.9 to 51.8	395.7 to 516.2	13.7%
Personnel hazard	16.2 to 18.9	30.2 to 45.3	303.5 to 449.2	10.5%
Supply chain hazard	5.4 to 8.1	18.7 to 28.7	183.3 to 280.8	6.3%
Physical and natural hazard	38.3 to 52.0	135.5 to 191.0	1,325.9 to 1,866.0	45.8%
Material risk	7.9 to 0.0	18.9 to 0.0	187.8 to 223.5	6.5%
Total critical data processing or storage assets	**116.6 to 150.1**	**296.9 to 402.3**	**2,895.7 to 4,136.2**	**100.0%**

The industry submissions also indicated the type of expenditure expected to be incurred. The allocation of cost between labour effort, capital and operating costs is provided in the table below. The analysis shows that 36.4% of one-off costs and 0.9% of ongoing costs are expected to be invested in capital. A relatively large share of costs are associated with labour effort (31.0% of one-

[354] For the purposes of calculating a total 10 year cost of compliance with the RMP framework, ongoing costs were assumed to commence in the year after the required implementation date (for example, for a rule requiring implementation within 2 years, the ongoing costs associated with the rule were assumed to start in year 3 of the 10 year period).

off costs and 85.0% of ongoing costs) with operating costs accounting for 32.6% of one-off costs and 14.2% of ongoing costs.

Expected one-off and ongoing costs by cost type for critical data processing or storage assets nationally

Cost Type	Costs			
	One-off ($ million)	One-off (%)	Ongoing (per year)	Ongoing (%)
Labour effort	36.2	31.0%	252.3	85.0%
Capital	42.5	36.4%	2.5	0.9%
Operating	38.0	32.6%	42.1	14.2%
Total critical data processing or storage assets	**116.6**	**100%**	**296.9**	**100.0%**

Benefits of option 2

The processing and storage of data is an integral part of everyday life, and is relied on by individuals, industry, and governments across Australia. Disruption to data processing or storage services can introduces significant costs to the economy. The risk management program framework aims to reduce the frequency and impact of any disruption to data storage and processing assets and, as such, its primary benefit is to avoid the incidents that may otherwise disrupt service and cause economic loss.

Economic impacts of disruptions to data storage and processing

Disruption to data storage and processing will affect industry and its customers, businesses, and households. Such disruptions can have costly immediate and longer-term impacts on the Australian economy. The immediate impacts of a data storage or processing outage are those associated with loss of access to data storage or processing, such as:

- Lost economic output (e.g. provision of dependent goods and services may cease);
- Lost productivity (e.g. workers may be idle whilst continuing to receive wages);
- Lost wages (e.g. workers may be sent home or unable to go to work);
- Increased cost of production if switching to a substitute service (e.g. an alternative data storage or processing service).

Computable General Equilibrium (CGE) modelling was used to illustrate how costly data storage and processing disruptions could potentially be by examining a hypothetical shock (i.e. a data storage and processing asset is affected by an incident with impacts on users) and an associated increase in input costs (i.e. an increase in the cost of the data storage and processing service). The advantage of using a CGE approach is that both the direct and indirect (i.e. flow-on) economic impacts of a data outage event can be quantified.[355]

[355] Direct economic impacts refer to the 'first-round' effects that occur directly as a result of an incident, while indirect economic impacts refer to flow-on effects to the economy due to supply chain linkages and other feedback responses by all economic agents (e.g., households, businesses).

Modelling Approach

To analyse the direct and indirect economic impacts of unplanned disruption to a data processing or storage service, a CGE approach was used to model 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.

The modelling framework is suited to analysing the economic impact of a data storage or processing disruption 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 disruption incident and the rest of the economy in a framework that combines detailed historical data with fundamental economic theory.

Scenarios

The CGE modelling provided estimates regarding how sensitive the Australian economy is to a shock to the data storage or processing system. This analysis was undertaken by deriving a set of hypothetical modelling scenarios based on assumptions about the intensity of a disruption to a data processing or storage asset, with the initial impact calibrated as reduction in the quantity of data supplied and the normalised insurance costs as a result of an event. The hypothetical scenarios were informed by studies of major events, which are discussed below.

Case studies

The case studies provided in the table below provide a basis for modelling hypothetical, but comparable disruptions, in an economy-wide model and contextualising the results of that modelling.

Incident	Summary of incident
Former employee attacks Cisco Systems (2018)	In September 2018, a former Cisco employee accessed Cisco Systems' cloud infrastructure, hosted by Amazon Web Services, without Cisco's permission. The former employee, during their unauthorised access, was successful in deleting 456 virtual machines from Cisco's WebEx Teams application. This resulted in more than 16,000 WebEx Teams accounts to be shut down for up to two weeks, forcing Cisco to spend approximately $1.4 million in employee time to restore the damage and refund over $1 million to affected customers.
Data centre hack on NordVPN(2018)	In March 2018, popular virtual private network provider NordVPN was hacked. The attacker gained access by exploiting an insecure remote management system. The ongoing impacts of the attack were minimal, with NordVPN stating that the compromised server did not contain any user activity logs, and with no compromise of usernames of passwords.
Melbourne Google Cloud experiences outage (2021)	In August 2021, Google's newest cloud region ('australia-southeast2'), located in Melbourne, experienced a 1 hour 30 minute outage due to a transient voltage issue, forcing network hardware to be rebooted. The disruption affected a total of 23 of Google's cloud services used by individuals and businesses alike, including Cloud Run, Cloud Filestore and Cloud SQL.
Kaseya ransomware attack (2021)	In 2021, IT services company Kaseya was hit by a ransomware attack perpetrated by Russian-based hacking group REvil. The attack directly and indirectly affected a large number of businesses globally. The hackers demanded approximately AU$92.9 million in Bitcoin be paid to provide a decryption tool to allow businesses to unlock their affected systems.

These case studies highlight that disruptions to data storage and processing services inflict substantial direct and indirect costs on firms and households alike. Businesses bore the brunt of the damage across all case studies, mostly through lost income and productivity. The nature of the

data processing and storage sector means that disruptions to data storage and processing services can affect large swathes of the economy as a flow-on effect.

For the purposes of modelling the cost of avoided future incidents in Australia, two incidents were selected to be simulated. The Cisco Systems attack was selected to be simulated due to the availability of sufficient information about its direct impact on customers to support the modelling. As the attack was limited to a single entity in what is a large sector, this incident is considered a low risk scenario. As a result of the attack, approximately 16,000 WebEx Teams accounts were shut down for up to two weeks, with approximately $1.4 million of employee time spent rectifying the damage and approximately $1 million paid as refunds to affected customers.

The Kaseya ransomware attack is selected as another baseline scenario to be modelled. The Kaseya attack demonstrates the potentially far-reaching consequences of a cyber-attack in the sector where essential services are reliant on services vulnerable to compromise by ransomware or other such threats. The Kaseya incident is treated as the moderate risk scenario. Despite the high degree of uncertainty about the scale of the incident and impacts on Kaseya, its direct customers and the indirectly affected entities, it is reasonable to assume that another similar attack on an organisation with a larger or more vulnerable customer base could produce a more severe outcome in terms of economic impact. The ransom demanded by the hacking group, AU$92.9 million, is treated as the total economic cost of the scenario for the purposes of benefits analysis. This figure does not take into account the financial impacts on affected businesses as a result of reduced or impacted operations

The use of actual events as a risk point of comparison is important, because it ensures the benefits analysis is grounded in reality. A framework for considering the potential impacts of Australian data storage or processing outages following failure of critical infrastructure is provided in the table below.

Framework for scenario development and sensitivity analysis

	Severe scenario	Moderate scenario	Low scenario
Intensity of event	200% of moderate scenario	Kaseya ransomware attack (2021)	Former employee targets Cisco Systems (2018)

As stated above, there is a rationale for a more severe scenario than experienced in the Kaseya ransomware attack, which the complexity of the scenarios that could occur. As noted above, the economic impact of an incident will vary due to a range of factors including the nature of an attack, the type and number of customers affected, as well as the timing and the duration of disruption. The defined scenarios and subsequent benefits analysis are based on a deliberately conservative approach to ensure the severe scenario remains demonstrably plausible.

A summary of the economic impact of each scenario is provided in the table below. A break-even analysis of these benefits compared to the total estimated cost of the risk management program framework is also included in the table. This break-even analysis is expressed as the number of incidents that would need to be avoided in order for the benefits (that is, the avoided costs) of the risk management program framework to equal the costs of implementation and compliance.

Summary of benefits scenarios

	Scenario 1 (Severe), $ million	Scenario 2 (Moderate), $ million	Scenario 3 (Low), $ million
Direct avoided costs	196.0	98.0	2.4
Indirect avoided costs	-	-	2.2
Total avoided cost to the	196.0	98.0	4.6

economy of the incident			
Approximate number of avoided incidents per annum required for a net benefit	3.8	7.5	160.1

As noted above in the cost of option 2, the total direct ongoing cost for option 2 is expected to be $296.9 million per annum plus direct one-off costs of $116.6 million. However, the cost of the risk management program framework would also have other indirect costs flowing from increased prices for data storage or processing services passed onto consumers from the framework's implementation.

After considering the economy-wide impact of this change to the cost of providing data storage or processing, the total economic cost of the regulatory changes, including direct and indirect costs would be approximately $738.0 million per year.[356] In order for the regulatory changes to generate a net benefit, the proposed risk management program framework would need to contribute to the prevention of approximately 165 low scenario incident approximately every year, approximately 8 moderate scenario incidents every year or approximately 4 severe scenarios every year to generate a net benefit.

In terms of the feasibility of achieving a net benefit based on these numbers of incidents, the scale of the sector and likelihood of incidents occurring should be considered. The Department estimates that the number of responsible entities for critical data storage or processing assets exceeds 300. In addition, the increasing frequency of incidents as described in section 1.1 makes the proposed risk management program framework more certain over time to exceed the anticipated costs. The examples referred to in that section demonstrate the increasing need for adequate protections for the security and resilience of critical data storage or processing assets, and the increased likelihood that the benefits of the draft risk management program framework will exceed the costs outlined in this section.

It is important to note that the economic analysis of the above scenarios may not incorporate all direct avoided costs incurred by all future incidents. A range of direct costs in addition to what has been modelled could be experienced, including costs associated with repair of physical assets, legal or regulatory costs.

Assessment of likely net benefit

The likely benefits of option 2 will be at least (and are expected to be more than) the costs of the regulation. This is primarily because, as described above and throughout this RIS, the frequency and severity of all hazard risks for critical data storage and processing assets are growing. The low baseline scenario is an incident which affected a single entity and its customers – an incident of this magnitude or greater could affect any business in the sector. Given there are estimated to be in excess of 300 responsible entities of varying size in Australia, the probability that incidents will occur in a significant number of these entities is high.[357] The moderate baseline scenario demonstrates the interconnected nature of the sector and cascading effects of a disruption to one

[356] The total economic cost (being direct and indirect costs) was determined using the same CGE model approach used to estimate the benefits scenarios above. Total economic cost was determined by the CGE model and was based on an assumed economic shock equal to the cost of the draft risk management program framework (being a one-off cost of $116.6 million and an ongoing cost of $296.9 million). This resulted in a total economic impact of $738.0 million per year for the moderate scenario.

CGE modelling is a whole-of-economy approach that represents the Australian 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. In this context, indirect costs refer to flow-on costs to the economy due to supply chain linkages and other feedback responses by all economic agents (e.g. households, businesses), including those due to changes in prices or a decline in production caused by the absence of gas supply.

[357] The Department estimates that the number of responsible entities exceeds 300 based off the proposed asset definition.

or more critical services upon which essential services rely. The inherent uncertainty around financial impacts of these types of incidents introduces a level of complexity when trying to understand specifics, but it can be assumed that financial implications are large or larger than what is considered in the benefits model

The increasing severity and frequency of similar incidents, particularly in the context of growing cybersecurity incidents, represents a risk to the whole economy. The potential economic consequences of disruption incidents in this sector are broad and uncertain. The increasing frequency of incidents, as described above and throughout the RIS, makes the proposed risk management program framework more likely to exceed the anticipated costs over time.

Further, through pursuit of option 2, the identification, mitigation and remediation of such hazards, should they occur, will be improved through:

- Lowering the material risk of hazards and subsequent impacts of those hazards, as they manifest for critical data storage or processing assets;
- Ensuring that adoption of the risk management program framework for critical data storage or processing assets is reasonable and proportionate to the purpose of the program;
- Avoiding regulatory duplication and facilitating a coordinated uplift in responsible entities' compliance with relevant standards; and
- Improving Government's visibility over the security and resilience of critical data storage or processing assets.

Overall, these factors and the specific costs and benefits described above mean the likely net benefit associated with option 2 is high.

Appendix U: Detailed costing information for critical broadcasting assets and critical domain name systems

The costing and subsequent benefit analysis process for critical broadcasting assets and critical domain name systems has been undertaken at a sector (communications) level. This is due to the small number of responsible entities in each asset class (two and one respectively).

Costing process completed by responsible entities in the communications sector

Cost submissions were received from 2 responsible entities for critical broadcasting assets. This represented 100.0% of the total critical broadcasting asset market. Cost submissions were received from 1 responsible entity for critical domain name system assets. This represented 100.0% of the total critical domain name system asset market.

Likely net benefit – option 2

The following section details the costs and benefits associated with option 2 (the regulatory option), before assessing the overall likely net benefit presented by this option.

Costs of option 2

There are multiple factors affecting the regulatory burden for each entity, including their existing risk management practices and capabilities, the nature of the critical assets they operate and the size of their operations. In collecting cost information from entities across critical broadcasting and critical domain name system assets, this variance in cost impact has been captured and reflected in the estimates of total cost across critical broadcasting assets included in this RIS.

When estimating the cost of compliance with option 2, critical broadcasting asset entities provided both an expected and a high-cost estimate. The high-cost estimate was provided as a way to measure the uncertainty associated with their estimates and the highest feasible cost of option 2. The expected estimate was used as the basis for determining the net benefit of option 2 in section 4.

Using the expected and the high estimate as a range, the cost of compliance is as follows:

- A one-off regulatory cost of between $2.1 (expected) and $3.5 million (high estimate), across critical broadcasting and domain name systems assets nationally; and
- An ongoing cost of between $1.5 (expected) and $2.4 million (high estimate) per year, across critical broadcasting and domain name systems assets nationally.

The cost of regulation will be borne by entities responsible for critical broadcasting assets who meet the relevant thresholds. Community organisations and individuals will not be directly affected but there will likely be indirect costs passed onto consumers. For the purposes of this RIS, the cost of regulation in the table below will only include the initial costs associated with regulation[358]. The indirect cost to consumers and communities has been addressed in the economic analysis through consideration of indirect cost to the wider economy because of the proposed risk management program framework.

[358] Department of Prime Minister and Cabinet, 2020.

The average cost of compliance for each entity is estimated at $0.7 million in one-off costs and $0.5 million per year in ongoing costs.

Regulatory cost estimate

Cost Type	Costs ($ million)			
	Business	Community	Individuals	Total cost ($ million)
One-off	2.1 to 3.5	nil	nil	2.1 to 3.5
Ongoing (per year)	1.5 to 2.4	nil	nil	1.5 to 2.4

Note: There will be no direct costs to individuals and communities although price rises may reflect the increased cost of operations as a result of the proposed Risk Management Program framework.

Based on the industry submissions made during consultations, total regulatory costs will be highest for rules and obligations associated with addressing risk management program obligations in the Act. These costs represent approximately 43.6% of the total cost of implementing the risk management program framework. The cost associated with personnel hazards (15.5% of total cost) are less significant but remain material. The total regulatory cost by rule/obligation is set out in the table below.

Regulatory burden estimate by rule and obligation for critical broadcasting assets and critical domain name systems nationally

Rule / obligation	Costs (Expected and High)			
	One-off ($ million)	Ongoing (per year, $ million)	Total cost over 10 years ($ million) [359]	Expected estimate as percentage of total (%)
Risk management program obligations in the Act	1.0 to 1.9	0.7 to 1.2	7.1 to 12.9	43.6
General rules	0.1 to 0.2	0.2 to 0.2	1.6 to 2.0	9.7
RMP rules				
Cyber and information security hazard	0.2 to 0.2	0.2 to 0.2	1.6 to 2.1	10.2
Personnel hazard	0.4 to 0.6	0.2 to 0.4	2.5 to 4.3	15.5
Supply chain hazard	0.3 to 0.3	0.1 to 0.2	1.6 to 2.0	10.1
Physical and natural hazard	0.1 to 0.1	0.1 to 0.1	0.8 to 0.9	4.6
Material risk	0.1 to 0.1	0.1 to 0.1	1.0 to 1.0	6.2
Total critical broadcasting assets and critical domain name systems	**2.1 to 3.5**	**1.5 to 2.4**	**16.2 to 25.2**	**100.0**

[359] For the purposes of calculating a total 10 year cost of compliance with the risk management program framework, ongoing costs were assumed to commence in the year after the required implementation date (for example, for a rule requiring implementation within 2 years, the ongoing costs associated with the rule were assumed to start in year 3 of the 10 year period).

The industry submissions also indicated the type of expenditure expected to be incurred. The allocation of cost between labour effort, capital and operating costs is provided in the table below. The analysis shows that 27.5% of one-off costs and 9.2% of ongoing costs are expected to be invested in capital. A relatively small share of one-off costs are associated with labour effort (16.1% of one-off costs and 22.9% of ongoing costs) with operating costs being the largest component of one-off and ongoing costs (56.4% of one-off costs and 68.0% of total ongoing costs).

Expected one-off and ongoing costs by cost type for critical broadcasting assets and critical domain name systems nationally

Cost Type	Costs			
	One-off ($ million)	One-off (%)	Ongoing (per year)	Ongoing (%)
Labour effort	0.3	16.1	0.4	22.9
Capital	0.6	27.5	0.1	9.2
Operating	1.2	56.4	1.0	68.0
Total critical broadcasting assets	**2.1**	**100.0**	**1.5**	**100.0**

Benefits of option 2

A reliable continuous broadcasting service is central to Australia's prosperity. Further, disruption to broadcasting services can be a significant cost to the economy. The risk management program framework aims to reduce the frequency and impact of any disruption to supply and so its primary benefit is to avoid the incidents that may otherwise disrupt supply and cause economic loss.

Economic impacts of disruptions to broadcasting

Disruptions that affect critical broadcasting assets can subsequently disrupt ability to broadcast radio or television programming to businesses and households. These events can generate costly immediate and longer-term impacts on the Australian economy. The immediate impacts of a broadcasting outage are those associated with loss of access to broadcasting or increased broadcasting costs, such as:

- Disrupted economic activity (e.g. disruption of business operations or systems caused by a disruption to broadcasting services);
- Lost productivity as a result of disrupted economic activity (e.g. workers may be idle whilst continuing to receive wages); and
- Lost wages (e.g. workers may be sent home or unable to go to work).

One of the most severe impacts of a disruption to broadcasting services is disruption to emergency telecommunications arrangements, and by extension community safety arrangements, in times of crisis. This scenario was realised during the summer of 2020 where radio and television networks were affected by the bushfire crisis, including an ABC transmission site in the South Coast being completely burnt out and rendered unusable.

Economic impacts of disruptions to domain name systems

The fundamental impact of a disruption to domain name systems is reduced ability or inability to navigate the internet and access data online, which in turn can affect economic activity (e.g. e-commerce, business operations dependent on access to the internet). Such disruptions can have costly immediate and longer-term impacts on the economy. The immediate impacts of a disruption

to domain name systems are those associated with reduced ability or inability to navigate the internet or access data online and increased costs, such as:

- Reduced economic activity (e.g. inability to navigate internet disrupting e-commerce or inability to access data affecting business operations);
- Lost productivity as a result of reduced economic activity (e.g. workers may be idle whilst continuing to receive wages); and
- Lost wages (e.g. workers may be sent home or unable to go to work).

Computable General Equilibrium (CGE) modelling was used to illustrate how costly a disruption to critical assets in the communications sector could potentially be by examining a hypothetical supply shock (i.e. reduced broadcasting services are available to users) and an associated increase in input costs (i.e. an increase in the cost of broadcasting services). The advantage of using a CGE approach is that both the direct and indirect (i.e. flow-on) economic impacts of a power outage event can be quantified.

CGE Modelling Approach

A scenario based on a disruption to a critical broadcasting asset was selected due to the availability of information and quantitative evidence. To analyse the direct and indirect economic contributions of a broadcasting outage due to disruptions to critical infrastructure on the Australian economy, a CGE approach was used to model 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 a broadcasting outage 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 outage and the rest of the economy in a framework that combines detailed historical data with fundamental economic theory.

Scenarios

The CGE modelling provided estimates regarding how sensitive the Australian economy is to a shock to the broadcasting system. This analysis was undertaken by deriving a set of hypothetical modelling scenarios based on assumptions about the impact of a disruption to broadcasting services. The scope of the hypothetical scenarios was based on studies of major events which are discussed below.

Case studies

The case studies provided in the table below provide a basis for modelling hypothetical, but comparable outages, in an economy-wide model and contextualising the results of that modelling. Case studies have been chosen to provide insights into the economy-wide costs to households and businesses of large-scale and severe broadcasting outage disruption events.

As stated above, for the purposes of this benefit analysis, incidents that affected broadcasting assets are being considered due to greater availability of information and quantitative evidence. Disruptions to domain name systems have occurred in the past and are described in Appendix M.

Broadcasting outage case studies in Australia and globally

Incident	Summary of incident
Channel Nine cyber-attack (2021)	On 29 March 2021, the Nine Network became the target of Australia's largest cyber-attack on a media company. For more than 24 hours, the cyberattack affected digital production systems and impaired Channel Nine's ability to broadcast from its Sydney studios, forcing the network to relocate operations to its Melbourne studios. As a result of the attack, data and production systems were temporarily unavailable. Additionally, the cyber-attack impacted regular news bulletins and impeded the Australian Financial Review, The Sydney Morning Herald, and The Age's ability to publish. According to estimates, the cyber-attack on the network is expected to cost the network more than $1 million dollars, in addition to significant recovery expenses
France TV5Monde cyber-attack (2015)	In April 2015, TV5Monde, one of France's largest television networks with an international reach in more than 200 countries, experienced the largest cyberattack ever against a television network. Highly targeted malware was used to destroy the TV network's systems, and all 12 of its channels were taken off the air.[360] The network was accessed on 23 January 2015, and the attackers remained hidden for months while conducting reconnaissance of the network, which is a common method for cyber-attacks looking for weaknesses in the network and associated systems. The Network had a three-hour outage during which it was unable to generate news programming. Additionally, the hackers posted documents and messages on TV5Monde's Facebook page pretending to be the families of French soldiers participating in anti-Islamic State Group operations, as well as posting threats against the troops. The cost of the attack was 5 million Euro in 2015 (8 million AUD) and 11 million Euro (18 million AUD) over the next three years – a total of more than 16 million Euro (26 million AUD).[361]
ABC's south coast transmitter – Australia's summer bushfires (2020)	The Australian bushfires that devastated the South Coast of New South Wales (NSW) in the summer of 2020 caused widespread devastation and panic, as the transmitter in the region melted. Communications with residents in the community were impaired by the inability to receive or transmit radio coverage.[362] The transmitter equipment required months of repairs before it was completely operational again. The cost of restoring the infrastructure owned by BAI Communications Australia, which provides the broadcast towers to ABC on a commercial arrangement, was between $1.5 million and $2 million.[363]

These case studies highlight that disruptions to critical broadcasting assets can inflict substantial direct and indirect costs on firms and households alike. The Channel Nine cyberattack disrupted digital production systems for over 24 hours, requiring the network to relocate operations and costing an estimated $1 million. The France TV5Monde cyber-attack scenario involved the use of social engineering techniques to affect programming through use of a Trojan horse virus, with substantial costs over the next three years reaching approximately $26 million. The ABC's south coast transmitter was rendered completely unusable by extreme conditions leading to significant repair costs and impacting the ability for emergency communications to be broadcast in the surrounding area.

For the purposes of the modelling of the cost of avoided future incidents in Australia, the South Coast transmitter bushfire incident was used as the baseline (moderate) risk scenario. The use of an actual event as the baseline risk point of comparison is important because it ensures the benefits analysis is grounded in reality. The scale of the event is not theoretical and there is sufficient information about the event to support modelling. News media estimated the repair work

[360] Corera, 2016

[361] Ibid

[362] Lauder, Reardon, McCutcheon 2020

[363] Ibid

cost between $1.5 million and $2 million. To ensure the scenario is plausible benefits analysis has been undertaken with a deliberately conservative approach, and therefore has used the $1.5 million figure as the basis for direct costs.

A framework for considering the potential impacts of the broadcasting outage following failure of critical infrastructure is provided in the table below.

Framework for scenario development and sensitivity analysis

	Severe scenario	Moderate scenario	Low scenario
Intensity of event	200% of moderate scenario costs	ABC's south coast transmitter bushfire incident (2020)	50% of moderate scenario costs

The rationale for a more severe scenario than experienced in the south coast transmitter incident reflects the complexity of the scenarios that could occur. As noted above, the economic impact of an incident will vary due to a range of factors including the location of a disruption, the month and time of day at which the disruption occurs, the day of the week on which the disruption takes place and the duration of disruption. Accounting for an incident that has a greater economic impact than the south coast transmitter incident is necessary to reflect the possibility that a disruption of a similar scale could impact areas where there would be greater economic impact than in the south case incident. While an incident with a much greater impact than the severe scenario is conceivable, the defined scenarios and subsequent benefits analysis has taken a deliberately conservative approach to ensure the severe scenario remains demonstrably plausible.

A summary of the economic impact of each scenario is provided in the table below. Direct avoided costs refer to the financial costs directly incurred as a result of an incident, while indirect costs refer to flow-on costs to the economy due to supply chain linkages and other feedback responses by all economic agents (e.g., households, businesses). A break-even analysis of these benefits compared to the total estimated cost of the risk management program framework is also included in the table. This break-even analysis is expressed as the number of incidents that would need to be avoided in order for the benefits (that is, the avoided costs) of the risk management program framework to equal the costs of implementation and compliance.

Summary of benefits scenarios

	Scenario 1 (Severe), $ million	Scenario 2 (Moderate), $ million	Scenario 3 (Low), $ million
Direct avoided cost	3.9	2.0	1.0
Indirect avoided costs	3.6	1.8	0.9
Total avoided cost to the economy of the incident	**7.7**	**3.8**	**1.9**
Approximate number of avoided incidents per annum required for a net benefit	0.9	1.8	3.6

As noted above, the total direct ongoing cost for option 2 is expected to be $1.5 million per annum plus direct one-off costs of $2.1 million. However, the cost of the risk management program framework would also have other indirect costs flowing from increased prices passed onto consumers from the framework's implementation.

After considering the economy-wide impact of this change to the cost of providing broadcasting and domain name system services, the total economic cost of the regulatory changes, including direct and indirect costs would be approximately $6.8million per year.[364] In order for the regulatory changes to generate a net benefit, the proposed risk management program framework would need to contribute to the prevention of approximately 3 low scenario incidents every year, approximately 2 moderate scenario incidents every year or approximately 1 severe scenario every year to generate a net benefit.

It is important to note that the economic analysis of the above scenarios does not incorporate all direct avoided costs incurred by all future incidents. The avoided costs included are only those which were directly and immediately incurred as a result of the south coast transmitter incident. In the broader context of a potential future disruption, in addition to the above estimate of benefits would be the avoided costs of recovery (repair costs, costs of resulting mitigations) from high value, specific circumstances which were not experienced during the south coast transmitter event. Consequently, the moderate case of the south coast transmitter incident is not likely to be the worst-case incident and an incident of the same scale in terms of broadcasting disruption could have a greater impact if it occurred in other locations.

Further, the increasing frequency of incidents as described in section 1.1 makes the proposed risk management program framework more certain over time to exceed the anticipated costs. The examples referred to in that section demonstrate the increasing need for adequate protections against the security and resilience of critical broadcasting assets, and the increased likelihood that the benefits of the draft risk management program framework will exceed the costs outlined in this section.

Assessment of likely net benefit

The likely benefits of option 2 will be at least (and are expected to be more than) the costs of the regulation. This is primarily because, as described above and throughout this RIS, the frequency and severity of all hazard risks for critical broadcasting assets and critical domain name systems are growing. While some events of the magnitude described in this RIS 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, as described above, makes the proposed risk management program framework more likely to exceed the anticipated costs over time.

Further, through pursuit of option 2, the identification, mitigation and remediation of such hazards, should they occur, will be improved through:

- Lowering the material risk of hazards and subsequent impacts of those hazards, as they manifest for critical broadcasting assets and critical domain name systems;
- Ensuring that adoption of the risk management program framework for critical broadcasting assets and critical domain name systems is reasonable and proportionate to the purpose of the program;

[364]The total economic cost (being direct and indirect costs) was determined using the same CGE model approach used to estimate the benefits scenarios above. Total economic cost was determined by the CGE model based on an assumed economic shock equal to the cost of the draft risk management program framework (being a one-off cost of $2.1 million and an ongoing cost of $1.5 million). This was a total economic impact of $6.8 million per year for the moderate scenario.

CGE modelling is a whole-of-economy approach that represents the Australian 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. In this context, indirect costs refer to flow-on costs to the economy due to supply chain linkages and other feedback responses by all economic agents (e.g. households, businesses), including those due to changes in prices or a decline in production caused by the absence of broadcasting supply.

- Avoiding regulatory duplication and facilitating a coordinated uplift in responsible entities' compliance with relevant standards; and
- Improving Government's visibility over the security and resilience of critical broadcasting assets and critical domain name systems.

Overall, these factors and the specific costs and benefits described above mean the likely net benefit associated with option 2 is high.

Appendix V: Detailed costing information for critical payment system assets

Costing process completed by responsible entities for critical payment system assets

Cost submissions were received from 2 responsible entities for critical payment system assets. This represented approximately 32.2% of the total critical payment system asset market.

Likely net benefit – option 2

The following section details the costs and benefits associated with option 2 (the regulatory option), before assessing the overall likely net benefit presented by this option.

Costs of option 2

There are multiple factors affecting the regulatory burden for each entity, including their existing risk management practices and capabilities, the nature of the critical payment systems they operate and the size of their operations. In collecting cost information from entities across critical payment systems, this variance in cost impact has been captured and reflected in the estimates of total cost across critical payment system assets included in this RIS.

When estimating the cost of compliance with option 2, critical payment systems asset entities provided both an expected and a high-cost estimate. The high-cost estimate was provided as a way to measure the uncertainty associated with their estimates and the highest feasible cost of option 2. The expected estimate was used as the basis for determining the net benefit of option 2 in section 4.

Using the expected and the high estimate as a range, the cost of compliance is as follows:

A one-off regulatory cost of between $0.6 (expected) and $1.1 million (high estimate), across critical payment systems assets nationally; and

An ongoing cost of between $5.7 (expected) and $8.2 million (high estimate) per year, across critical payment systems assets nationally.

The average cost of compliance for each entity is estimated at $0.1 million in one-off costs and $1.4 million per year in ongoing costs.

The cost of regulation will be borne by entities responsible for critical payment systems who meet the relevant thresholds. Community organisations and individuals will not be directly affected but there will likely be indirect costs passed onto consumers. For the purposes of this RIS, the cost of regulation in the table below will only include the initial costs associated with regulation[365]. The indirect cost to consumers and communities has been addressed in the economic analysis through consideration of indirect cost to the wider economy as a result of the proposed RMP framework.

[365] Department of Prime Minister and Cabinet, 2020

Regulatory cost estimate

Cost Type	Costs ($ million)			
	Business	Community	Individuals	Total cost
One-off	0.6 to 1.1	Nil	Nil	0.6 to 1.1
Ongoing (per year)	5.7 to 8.2	Nil	Nil	5.7 to 8.2

Note: There will be no direct costs to individuals and communities although price rises may reflect the increased cost of operations as a result of the proposed RMP framework.

Based on the industry submissions made during consultations, total regulatory costs will be highest for rules and obligations associated with addressing material risk rules. These costs represent approximately 28.7% of the total cost of implementing the RMP framework. The cost associated with cyber and information security hazards (18.0% of total cost), RMP obligations in the Act (17.2% of total cost) and physical and natural hazard rules (14.4% of total cost) are less significant but remain material. Compliance costs associated with general rules, personnel hazards and supply chain hazards were the least costly aspects of the RMP framework, representing in total approximately 21.7% of costs in total. The total regulatory cost by rule/obligation is set out in the table below.

Regulatory burden estimate by rule and obligation for critical payment systems nationally

Rule / obligation	Costs (Expected and High)			
	One-off ($ million)	Ongoing (per year, $ million)	Total cost over 10 years ($ million) [366]	Expected estimate as percentage of total (%)
RMP obligations in the Act	0.1 to 0.2	1.0 to 1.5	9.2 to 13.6	17.2
General rules	0.0 to 0.0	0.5 to 0.8	4.9 to 7.3	9.1
RMP rules				
Cyber and information security hazard	0.2 to 0.4	1.0 to 1.5	9.7 to 14.2	18.0
Personnel hazard	0.0 to 0.1	0.2 to 0.2	2.1 to 2.1	3.9
Supply chain hazard	0.2 to 0.4	0.5 to 0.9	4.7 to 9.4	8.7
Physical and natural hazard	0.0 to 0.0	0.8 to 1.1	7.7 to 10.3	14.4
Material risk	0.0 to 0.0	1.6 to 2.2	15.4 to 20.6	28.7
Total critical payment systems assets	**0.6 to 1.1**	**5.7 to 8.2**	**53.7 to 77.4**	**100**

The industry submissions also indicated the type of expenditure expected to be incurred. The allocation of cost between labour effort, capital and operating costs is provided in the table below. The analysis shows that 14.1% of one-off costs and 0% of ongoing costs are expected to be invested in capital. A relatively small share of one-off costs is associated with labour effort (14.1%).

[366] For the purposes of calculating a total 10 year cost of compliance with the RMP framework, ongoing costs were assumed to commence in the year after the required implementation date (for example, for a rule requiring implementation within 2 years, the ongoing costs associated with the rule were assumed to start in year 3 of the 10 year period).

Labour effort is the largest component of ongoing costs with 86.0% of the total. Operating costs are the largest component of one-off costs (71.8% of total ongoing costs).

Expected one-off and ongoing costs by cost type for critical payment systems assets nationally

Cost Type	Costs			
	One-off ($ million)	One-off (%)	Ongoing (per year)	Ongoing (%)
Labour effort	0.1	14.1%	4.9	86.0%
Capital	0.1	14.1%	0.0	0.0%
Operating	0.4	71.8%	0.8	14.0%
Total critical payment system assets	**0.6**	**100.0**	**5.7**	**100.0**

Benefits of option 2

A reliable continuous payment systems supply is central to Australia's prosperity. Further, disruption to supply can be a significant cost to the economy. The RMP framework aims to reduce the frequency and impact of any disruption to supply and so its primary benefit is to avoid the incidents that may otherwise disrupt supply and cause economic loss.

Economic impacts of disruptions to payment systems supply

Damage to critical payment systems can subsequently disrupt businesses and households. These events can generate costly immediate and longer-term impacts on the Australian economy. The immediate impacts of a payment systems outage are those associated with loss of access to payment systems or increased cost of accessing payment systems services, such as:

- Lost economic activity (e.g. ability to conduct business may cease due to inability to process payment);
- Lost productivity (e.g. workers may be idle whilst continuing to receive wages);
- Lost wages (e.g. workers may be sent home or unable to go to work); and

CGE Modelling Approach

To analyse the direct and indirect economic contributions of a payment systems outage due to disruptions to critical infrastructure on the Australian economy, a CGE approach was used to model 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 a payment systems outage 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 outage and the rest of the economy in a framework that combines detailed historical data with fundamental economic theory.

Scenarios

The CGE modelling provided estimates regarding how sensitive the Australian economy is to a shock to the payment system ecosystem. This analysis was undertaken by deriving a set of hypothetical modelling scenarios based on assumptions about the impact of a disruption to payment systems services. The scope of the hypothetical scenarios was based on studies of real-world events which are discussed below.

Case studies

The case studies provided in the table below provide a basis for modelling hypothetical, but comparable outages, in an economy-wide model and contextualising the results of that modelling. Case studies have been chosen to provide insights into the economy-wide costs to households and businesses of large-scale and severe payment systems disruption events.

Payment systems disruption case studies in Australia and globally

Incident	Summary of incident
Major Banks Denial of Service Attack (2021)	Australia's major banks internet services and payment terminals, as well as those of other major Australian brands, experienced outages on 17 June 2021. The outage was due to an issue with technology company Akamai's distributed denial of service mitigation platform 'Prolexic'. Enduring impacts were minimal, but essential payment, travel and postal service caused inconvenience to customers.
Boxing Day Malfunctions (2018)	On Boxing Day 2018 Westpac and ANZ eftpos and mobile banking applications experienced significant malfunctions throughout the day, while Coles-Myer gift cards were unable to be accepted. ANZ and Coles-Myer were both able to restore services by Boxing Day evening, while Westpac's issues weren't resolved by the end of the day. The outages came on a day when Australians were expected to spend as much as $2.62 billion as considering Boxing Day sales.
NAB nationwide service outage (2018)	In early 2018, NAB experienced extended outages across its internet and mobile banking ATMs and eftpos, with disruptions lasting almost seven hours on a Saturday. The outage was caused by a power issue in the bank's mainframe in Melbourne. Compensation payments to businesses for losses incurred as a result of the outage totalled $7.4 million.

These three case studies highlight that payment systems disruptions inflict substantial direct and indirect costs on businesses and households alike. The Boxing Day 2018 third-party gift card provider incident, which occurred during one of the busiest shopping days of the year, shows the importance of contingency arrangements in the event of an outage. The 2021 DDoS attacks on major banks and other organisations, while limited in enduring impacts, highlight the importance of appropriate cyber mitigations and network redundancy to reduce the severity of DDoS attacks. The 2018 NAB service disruption demonstrates the range of potential risk vectors that can affect the ability of payments to be processed, with a physical power issue causing the incident and subsequent impacts for customers.

For the purposes of the modelling of the cost of avoided future incidents in Australia, the NAB service outage was used as the baseline (moderate) risk scenario. The use of an actual event as the baseline risk point of comparison is important because it ensures the benefits analysis is grounded in reality. The scale of the event is not theoretical and there is sufficient information about the event to support modelling. NAB paid out compensation totalling $7.4 million to affected customers following the incident.

It is noted that the selected baseline scenario affected an organisation which is not a proposed responsible entity within the critical financial market infrastructure (payment systems) asset class. The incident is appropriate to model as the real-world impacts to consumers, businesses and the

economy of an outage affecting the products of the proposed responsible entities would be comparable to that which was experienced in 2018 when NAB was the affected entity.

A framework for considering the potential impacts of a payment systems outage following failure of critical infrastructure is provided in the table below.

Framework for scenario development and sensitivity analysis

	Severe scenario	Moderate scenario	Low scenario
Intensity of event	200% of severe scenario	NAB service outage (2018)	50% of severe scenario

The rationale for considering less severe scenarios than experienced in the NAB service outage reflects the complexity of the scenarios that could occur. As noted above, the economic impact of an incident will vary due to a range of factors including the location of a disruption, the month and time of day at which the disruption occurs, the day of the week on which the disruption takes place and the duration of disruption. Accounting for an incident that has a lesser economic impact than the NAB service outage is necessary to reflect the possibility that a disruption of the same scale (in terms of a payment systems outage) could impact at a time when there would be lessened economic impact than in the NAB incident (which occurred on a Saturday, a busy trading day). While an incident with a much greater impact than the severe scenario is possible, the defined scenarios and subsequent benefits analysis has taken a deliberately conservative approach to ensure the severe scenario remains demonstrably plausible.

A summary of the economic impact of each scenario is provided in the table below. Direct avoided costs refer to the financial costs directly incurred as a result of an incident, while indirect costs refer to flow-on costs to the economy due to supply chain linkages and other feedback responses by all economic agents (e.g., households, businesses). A break-even analysis of these benefits compared to the total estimated cost of the RMP framework is also included in the table. This break-even analysis is expressed as the number of incidents that would need to be avoided in order for the benefits (that is, the avoided costs) of the RMP framework to equal the costs of implementation and compliance.

Summary of benefits scenarios

	Scenario 1 (Severe), $ million	Scenario 2 (Moderate), $ million	Scenario 3 (Low), $ million
Direct avoided cost	14.9	7.4	3.7
Indirect avoided costs	12.2	6.1	3.1
Total avoided cost to the economy of the incident	27.1	13.5	6.8
Approximate number of avoided incidents per annum required for a net benefit	0.4	0.9	1.7

As noted above, the total direct ongoing cost for option 2 is expected to be $5.7 million per annum plus direct one-off costs of $0.6 million. However, the cost of the RMP framework would also have other indirect costs flowing from increased payment systems prices passed onto consumers from the framework's implementation.

After considering the economy-wide impact of this change to the cost of providing payment systems, the total economic cost of the regulatory changes, including direct and indirect costs would be approximately $11.6 million per year.[367] In order for the regulatory changes to generate a net benefit, the proposed RMP framework would need to contribute to the prevention of approximately 1.7 low scenario incidents every year, 1 moderate scenario incidents every year or 0.4 severe scenarios every year to generate a net benefit.

It is important to note that the economic analysis of the above scenarios does not incorporate all direct avoided costs incurred by all future incidents. The avoided costs included are only those which were directly and immediately incurred as a result of the NAB service outage. In the broader context of a potential future disruption, in addition to the above estimate of benefits would be the avoided costs of recovery (repair costs, costs of resulting mitigations) from high value, specific circumstances which were not experienced during the NAB service outage. Consequently, the severe case of the NAB service outage is not likely to be a best- or worst-case incident and an incident of the same scale in terms of payment systems disruption could have a greater or lesser impact if it occurred in other locations or at other times.

Further, the increasing frequency of incidents as described in section 1.1 makes the proposed RMP framework more certain over time to exceed the anticipated costs. The examples referred to in that section demonstrate the increasing need for adequate protections against the security and resilience of critical payment systems, and the increased likelihood that the benefits of the draft RMP framework will exceed the costs outlined in this section.

Assessment of likely net benefit

The likely benefits of option 2 will be at least (and are expected to be more than) the costs of the regulation. This is primarily because, as described above and throughout this RIS, the frequency and severity of all hazard risks for critical payment systems are growing. While some events of the magnitude described in this RIS 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 high number of cybercrime incidents in the financial sector in particular (2,700 as reported by the ACSC in 2020-21)[368] and the increasing frequency of incidents, as described above, makes the proposed RMP framework more likely to exceed the anticipated costs over time.

Further, through pursuit of option 2, the identification, mitigation and remediation of such hazards, should they occur, will be improved through:

- Lowering the material risk of hazards and subsequent impacts of those hazards, as they manifest for critical payment systems;
- Ensuring that adoption of the RMP framework for critical payment systems is reasonable and proportionate to the purpose of the program;

[367] The total economic cost (being direct and indirect costs) was determined using the same CGE model approach used to estimate the benefits scenarios above. Total economic cost was determined by the CGE model based on an assumed economic shock equal to the cost of the draft RMP framework (being a one-off cost of $0.6 million and an ongoing cost of $5.7 million). This was a total economic impact of $11.6 million per year for the moderate scenario.

CGE modelling is a whole-of-economy approach that represents the Australian 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. In this context, indirect costs refer to flow-on costs to the economy due to supply chain linkages and other feedback responses by all economic agents (e.g. households, businesses), including those due to changes in prices or a decline in production caused by the absence of payment systems supply.

[368] ACSC 2021

- Avoiding regulatory duplication and facilitating a coordinated uplift in responsible entities' compliance with relevant standards; and
- Improving Government's visibility over the security and resilience of critical payment systems.

Overall, these factors and the specific costs and benefits described above mean the likely net benefit associated with option 2 is high.

Appendix Y: Detailed costing information for critical liquid fuel assets

No responsible entity for critical liquid fuel assets submitted an estimated cost of compliance. To estimate the cost of compliance for the liquid fuels sector, the average cost of compliance of similar sized entities in the critical gas sector was used as the base cost for liquid fuel entities. Critical gas asset entity submissions were used as the baseline as critical liquid fuels asset entities operate comparable businesses with similar assets, personnel and geography. The below analysis only focuses on the expected costs of the critical liquid fuels asset market.

Likely net benefit – option 2

The following section details the costs and benefits associated with option 2 (the regulatory option), before assessing the overall likely net benefit presented by this option.

Costs of option 2

The expected cost of compliance is as follows:

- A one-off regulatory cost of $35.8 million, across critical liquid fuel assets nationally; and
- An ongoing cost of $10.5 million per year, across critical liquid fuel assets nationally.

The average expected cost of compliance for each entity was estimated at $8.9 million in one-off costs and $2.6 million per year in ongoing costs.

The cost of regulation will be borne by entities responsible for critical liquid fuel assets who meet the relevant thresholds. Community organisations and individuals will not be directly affected but there will likely be indirect costs passed onto consumers. For the purposes of this RIS, the cost of regulation in the table below will only include the initial costs associated with regulation[369]. The indirect cost to consumers and communities has been addressed in the economic analysis through consideration of indirect cost to the wider economy as a result of the proposed RMP framework.

Regulatory cost estimate

Cost Type	Costs ($ million)			
	Business	Community	Individuals	Total cost
One-off	35.8	Nil	Nil	35.8
Ongoing (per year)	10.5	Nil	Nil	10.5

Note: There will be no direct costs to individuals and communities although price rises may reflect the increased cost of operations as a result of the proposed RMP framework.

Based on the industry submissions made during consultations, total regulatory costs will be highest for rules and obligations associated with addressing risk RMP obligations in the Act. These costs represent approximately 27.4% of the total cost of implementing the RMP framework. The cost associated with supply chain hazards (22.8% of total cost), cyber and information security hazards (17.1% of total cost) and material risk rules (12.5% of total cost) are less significant but remain material. Compliance costs associated with general rules, personnel hazards and physical and

[369] Department of Prime Minister and Cabinet, 2020

natural hazards were the least costly aspects of the RMP framework, representing in total approximately 20.2% of costs in total. The total regulatory cost by rule/obligation is set out in the table below.

Regulatory burden estimate by rule and obligation for critical liquid fuel nationally

Rule / obligation	Costs (Expected)			
	One-off ($ million)	Ongoing (per year, $ million)	Total cost over 10 years ($ million) [370]	Expected estimate as percentage of total (%)
RMP obligations in the Act	2.1	0.8	9.2	7.0%
General rules	1.2	0.3	3.6	2.8%
RMP Rules				
Cyber and information security hazard	10.2	3.3	37.8	28.8%
Personnel hazard	2.9	1.3	15.5	11.8%
Supply chain hazard	6.3	1.8	23.6	17.9%
Physical and natural hazard	11.5	2.1	31.3	23.8%
Material risk	1.6	0.9	10.5	8.0%
Total critical liquid fuel assets	**35.8**	**10.5**	**131.5**	**100.0%**

Benefits of option 2

A reliable continuous liquid fuels supply is central to Australia's prosperity. Further, disruption to supply can be a significant cost to the economy. The risk management program framework aims to reduce the frequency and impact of any disruption to supply and so its primary benefit is to avoid the incidents that may otherwise disrupt supply and cause economic loss.

Economic impacts of disruptions to liquid fuels supply

Disruption to the production, storage and distribution of liquid fuels will adversely impact the liquid fuels industry and its customers, businesses and households. Such disruptions can have costly immediate and longer-term impacts on the Australian economy. The immediate impacts of a disruption to liquid fuels supply are those associated with loss of access to the product or increased costs, such as:

- Lost production (e.g. production of goods and services may cease);
- Lost productivity (e.g. workers may be idle whilst continuing to receive wages);
- Lost wages (e.g. workers may be sent home or unable to go to work);
- Increased cost of production if switching to a substitute source of energy (e.g. backup generator).

[370] For the purposes of calculating a total 10 year cost of compliance with the RMP framework, ongoing costs were assumed to commence in the year after the required implementation date (for example, for a rule requiring implementation within 2 years, the ongoing costs associated with the rule were assumed to start in year 3 of the 10 year period).

Computable General Equilibrium (CGE) modelling was used to illustrate how costly liquid fuels disruptions could potentially be by examining a hypothetical supply shock (i.e. less liquid fuel available to users) and an associated increase in input costs (i.e. an increase in the cost of liquid fuels). The advantage of using a CGE approach is that both the direct and indirect (i.e. flow-on) economic impacts of a liquid fuels outage event can be quantified.[371]

Modelling Approach

To analyse the direct and indirect economic impacts of unplanned outages in the liquid fuels network due to disruptions to critical infrastructure on the Australian economy, a CGE approach was used to model 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.

The modelling framework is suited to analysing the economic impact of a liquid fuels supply disruption 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 liquid fuels disruption incident and the rest of the economy in a framework that combines detailed historical data with fundamental economic theory.

Scenarios

The CGE modelling provided estimates regarding how sensitive the Australian economy is to a shock to the liquid fuels system. This analysis was undertaken by deriving a set of hypothetical modelling scenarios based on assumptions about the intensity of a liquid fuels outage, with the initial impact calibrated as reduction in the quantity of liquid fuels supplied and the normalised insurance costs as a result of an event. The hypothetical scenarios were informed by studies of major events, which are discussed below.

Case studies

The case studies provided in the table below provide a basis for modelling hypothetical, but comparable outages, in an economy-wide model and contextualising the results of that modelling. Case studies have been chosen to provide insights into the economy-wide costs to households and businesses of large-scale and severe liquid fuels disruption events. An example which affected the gas sector is included, the Varanus Island disruption, due to the inherent similarities between the sectors.

Incident	Summary of incident
Varanus Island disruption, Western Australia	In June 2008, a major disruption to the natural gas supply in Western Australia occurred due to the rupture of a corroded pipeline and the subsequent explosion at a processing plant on Varanus Island, off the state's north west coast. The Apache Energy's plant was shut down, reducing Western Australia's gas supply by around 30% for over two months. Gas spot prices increased sharply, and several mining and industrial companies were forced to curtail

[371] Direct economic impacts refer to the 'first-round' effects that occur directly as a result of an incident, while indirect economic impacts refer to flow-on effects to the economy due to supply chain linkages and other feedback responses by all economic agents (e.g., households, businesses).

(2008)	production. Some electricity generators switched to emergency diesel stocks, and coal fired power plants that had been closed were also brought back online.[372]
Colonial Pipeline Cyber Attack (2021)	On May 7 2021 the Colonial Pipeline, the largest in the American oil pipeline system, was hit by the largest ransomware cyber-attack in the liquid fuels industry. The attack affected the pipeline's computerised equipment and provoked the shutdown of operations for five days. Colonial Pipeline paid a ransom of around US$5 million (AUD$6.49 million) to restore the system and recover stolen data.

These case studies highlight that liquid fuels outages inflict substantial direct and indirect costs on firms and households alike. Businesses bore the brunt of the damage across all case studies, mostly through lost income and productivity.

For the purposes of the modelling of the cost of avoided future incidents in Australia, the Varanus Island disruption was selected to be simulated due to the availability of sufficient information about its direct impact on liquid fuels supply to support the modelling. As the gas and liquid fuels sectors are similar in terms of the types of equipment and infrastructure used in production and distribution, it was assessed that the scenario, while initially simulated for the gas benefit analysis, was appropriate for this analysis also. Given the major magnitude of damages, this incident is considered a severe risk scenario. The use of an actual event as a risk point of comparison is important because it ensures the benefits analysis is grounded in reality. The plant, which normally supplied a third of the state's gas, was closed for almost two months. Supply from the plant partially resumed in late August. By mid-October, gas production was running at two-thirds of normal capacity with 85% of fully capacity restored by December 2008. It is estimated that approximately 40-50 Petajoules, or 4-5% of total national gas supply, was lost in 2008.[373] According to the Insurance Council of Australia, the normalised insurance losses were about $279 million (in 2011 dollars) or $340 million (in 2021 dollars).[374] The estimate of insurance losses should be interpreted with caution – a senate inquiry into matters relating to the explosion indicated that the relatively modest insurance impact reflected most companies choosing not to take out business disruption insurance, and in several cases, policies only allowing a claim if gas supply was completely cut off rather than just being reduced or subject to high deductibles.[375]

In addition to the Varanus Island example, the Colonial Pipeline cyber-attack incident has been simulated as the low-risk scenario. The direct cost of the incident able to be modelled includes the ransom paid to restore the system and recover stolen data but does not include other direct costs as a result of the fuel shortage caused by the incident. As full costs are likely not captured, the incident is treated as the low-risk scenario for the purposes of benefits analysis.

A framework for considering the potential impacts of Australian liquid fuels outages following failure of critical infrastructure is provided in the table below.

Framework for scenario development and sensitivity analysis

	Severe scenario	Moderate scenario	Low scenario
Intensity of event	Varanus Island disruption (2008)[376]	50% of severe scenario liquid fuels supply loss	Colonial Pipeline ransomware attack (2021)

[372] Government of Western Australia – Office of Energy, *Gas Supply and Emergency Management Committee – Report to Government,* September 2009.

[373] This is estimated using the timeline of the Varanus Island event and information about the quantity of gas demand and production sourced from the State of the Energy Market 2008 by Australian Energy Regulator.

[374] Australian Institute for Disaster Resilience, *Varanus Island gas explosion 2008*, June 2008.

[375] The Senate Standing Committee on Economics, *Matters relating to the gas explosion at Varanus Island, Western Australia,* December 2008.

[376] Total avoided cost of the incident to the economy is based on a conservative economy-wide impact estimation of an incident that results in a 4-5% gas supply shortage in annual terms to the national economy and the estimated normalised insurance cost of about $340 million (in 2021 dollars).

The rationale for a more severe scenario than experienced in the Varanus Island incident reflects the complexity of the scenarios that could occur. As noted above, the economic impact of an incident will vary due to a range of factors including the location of a disruption, as well as the timing and the duration of disruption. While an incident with a much greater impact than the severe scenario is conceivable, the defined scenarios and subsequent benefits analysis are based on a deliberately conservative approach to ensure the severe scenario remains demonstrably plausible.

A summary of the economic impact of each scenario is provided in the table below. A break-even analysis of these benefits compared to the total estimated cost of the risk management program framework is also included in the table. This break-even analysis is expressed as the number of incidents that would need to be avoided in order for the benefits (that is, the avoided costs) of the risk management program framework to equal the costs of implementation and compliance.

Summary of benefits scenarios

	Scenario 1 (Severe), $ million	Scenario 2 (Moderate), $ million	Scenario 3 (Low), $ million
Total avoided cost to the economy of the incident	1,913.0	1,001.0	14.5
Approximate number of avoided incidents per annum required for a net benefit	Less than 0.1	Less than 0.1	1.1

As noted above in the cost of option 2, the total direct ongoing cost for option 2 is expected to be $10.5 million per annum plus direct one-off costs of $35.8 million. However, the cost of the risk management program framework would also have other indirect costs flowing from increased gas prices passed onto consumers from the framework's implementation.

After considering the economy-wide impact of this change to the cost of providing liquid fuels, the total economic cost of the regulatory changes, including direct and indirect costs would be approximately $15.9 million per year.[377] In order for the regulatory changes to generate a net benefit, the proposed risk management program framework would need to contribute to the prevention of approximately 1 low scenario incident approximately every year, approximately 1 moderate scenario incident every 60 years or approximately 1 severe scenario every 120 years to generate a net benefit.

It is important to note that the economic analysis of the above scenarios may not incorporate all direct avoided costs incurred by all future incidents. In the broader context of a potential future disruption, in addition to the above estimate of benefits would be the avoided costs of recovery (repair costs, costs of resulting mitigations, productivity loss due to attending to legal ramifications, intangible costs on the environment, health and wellbeing, loss of reputation etc.) from high value, specific circumstances which were not experienced during the Varanus Island event. For example,

[377]The total economic cost (being direct and indirect costs) was determined using the same CGE model approach used to estimate the benefits scenarios above. Total economic cost was determined by the CGE model and was based on an assumed economic shock equal to the cost of the draft risk management program framework (being a one-off cost of $35.8 million and an ongoing cost of $10.5 million). This resulted in a total economic impact of $15.9 million per year for the moderate scenario.

CGE modelling is a whole-of-economy approach that represents the Australian 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. In this context, indirect costs refer to flow-on costs to the economy due to supply chain linkages and other feedback responses by all economic agents (e.g. households, businesses), including those due to changes in prices or a decline in production caused by the absence of gas supply.

the Enbridge incident in Canada forced 125 residents within a 2km radius of the explosion site to evacuate, and the Longford incident in 1998 caused two deaths and eight injuries.

Further, the increasing frequency of incidents as described in section 1.1 makes the proposed risk management program framework more certain over time to exceed the anticipated costs. The examples referred to in that section demonstrate the increasing need for adequate protections against the security and resilience of critical liquid fuel assets, and the increased likelihood that the benefits of the draft risk management program framework will exceed the costs outlined in this section.

Assessment of likely net benefit

The likely benefits of option 2 will be at least (and are expected to be more than) the costs of the regulation. This is primarily because, as described above and throughout this RIS, the frequency and severity of all hazard risks for critical liquid fuel assets are growing. While some events of the magnitude described in this RIS 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, as described above, makes the proposed risk management program framework more likely to exceed the anticipated costs over time.

Further, through pursuit of option 2, the identification, mitigation and remediation of such hazards, should they occur, will be improved through:

- Lowering the material risk of hazards and subsequent impacts of those hazards, as they manifest for critical liquid fuels assets;
- Ensuring that adoption of the risk management program framework for critical liquid fuels assets is reasonable and proportionate to the purpose of the program;
- Avoiding regulatory duplication and facilitating a coordinated uplift in responsible entities' compliance with relevant standards; and
- Improving Government's visibility over the security and resilience of critical liquid fuels assets.

Overall, these factors and the specific costs and benefits described above mean the likely net benefit associated with option 2 is high.

Appendix Z: Detailed costing information for critical hospital assets

Cost submissions were received from 23 responsible entities for critical hospital assets. This represented approximately 90% of the ICU bed capacity of critical hospital assets.

Likely net benefit – option 2

The following section details the costs and benefits associated with option 2 (the regulatory option), before assessing the overall likely net benefit presented by this option.

Costs of option 2

When estimating the cost of compliance with option 2, critical hospitals asset entities provided both an expected and a high-cost estimate. The high-cost estimate was provided as a way to measure the uncertainty associated with their estimates, and the highest feasible cost of option 2. The expected estimate was used as the basis for determining the net benefit of option 2 in section 4.

Using the expected and the high estimate as a range, the cost of compliance is as follows:

- A one-off regulatory cost of between $342.6 (expected) and $536.8 million (high estimate), across critical hospital assets nationally; and
- An ongoing cost of between $265.1 (expected) and $396.0 million (high estimate) per year, across critical hospital assets nationally.

The average expected cost of compliance for each entity is estimated at $13.0 million in one-off costs and $10.1 million per year in ongoing costs.

The cost of regulation will be borne by entities responsible for critical hospital who meet the relevant thresholds. Community organisations and individuals will not be directly affected but there will likely be indirect costs passed onto consumers. For the purposes of this RIS, the cost of regulation in the table below will only include the initial costs associated with regulation.[378] The indirect cost to consumers and communities has been addressed in the economic analysis through consideration of indirect cost to the wider economy as a result of the proposed RMP framework.

Regulatory cost estimate

Cost Type	Costs ($ million)			
	Business	Community	Individuals	Total cost
One-off	342.6 to 536.8	Nil	Nil	342.6 to 536.8
Ongoing (per year)	265.1 to 396.0	Nil	Nil	265.1 to 396.0

Note: There will be no direct costs to individuals and communities although price rises may reflect the increased cost of operations as a result of the proposed RMP framework.

Based on the industry submissions made during consultations, total regulatory costs will be highest for rules and obligations associated with addressing cyber and information security hazards. These costs represent approximately 49.6% of the total cost of implementing the RMP framework. The cost associated with personnel hazard rules (13.6% of total cost) and physical and natural hazard

[378] Department of Prime Minister and Cabinet, 2020

rules (11.3% of total cost) are less significant but remain material. Compliance costs associated with RMP obligations in the SLACIP Act, general rules, supply chain hazards and material risk rules were the least costly aspects of the RMP framework, representing in total approximately 25.4% of costs in total. The total regulatory cost by rule/obligation is set out in the table below.

Regulatory burden estimate by rule and obligation for critical hospital assets nationally

Rule / obligation	Costs (Expected and High)			
	One-off ($ million)	Ongoing (per year, $ million)	Total cost over 10 years ($ million) [379]	Expected estimate as percentage of total (%)
RMP obligations in the SLACIP Act	28.3 to 51.7	18.3 to 34.3	192.7 to 360.8	7.0
General rules	17.2 to 30.5	9.1 to 16.4	98.7 to 177.7	3.6
RMP Rules				
Cyber and information security hazard	170.1 to 243.2	136.7 to 198.8	1,358.9 to 1,973.8	49.6
Personnel hazard	39.1 to 69.2	35.1 to 49.0	372.6 to 534.3	13.6
Supply chain hazard	29.4 to 52.1	15.6 to 25.0	178.0 to 289.6	6.5
Physical and natural hazard	37.7 to 50.1	28.6 to 48.7	309.4 to 512.9	11.3
Material risk	20.9 to 40.0	21.7 to 23.8	227.1 to 265.7	8.3
Total critical hospital assets	**342.6 to 536.8**	**265.1 to 396.0**	**2,737.3 to 4,114.9**	**100.0**

The industry submissions also indicated the type of expenditure expected to be incurred. The allocation of expected cost between labour effort, capital and operating costs is provided in the table below. The analysis shows that 39.9% of one-off and 39.7% of ongoing costs are expected to be invested in capital. A relatively small share of costs is associated with labour effort for one-off and ongoing costs (21.2% for one-off costs and 20.5% for ongoing costs). Operating costs are the account for 39.8% of ongoing costs and 38.9% of one-off costs.

Expected one-off and ongoing costs by cost type for critical hospital assets nationally

Cost Type	Costs			
	One-off ($ million)	One-off (%)	Ongoing (per year)	Ongoing (%)
Labour effort	72.5	21.2	54.4	20.5
Capital	136.6	39.9	105.4	39.7
Operating	133.5	38.9	105.4	39.8

[379] For the purposes of calculating a total 10 year cost of compliance with the RMP framework, ongoing costs were assumed to commence in the year after the required implementation date (for example, for a rule requiring implementation within 2 years, the ongoing costs associated with the rule were assumed to start in year 3 of the 10 year period).

Total critical hospital assets	**342.6**	**100.0**	**265.1**	**100.0**

Benefits of option 2

A reliable continuous hospital system is central to Australia's prosperity. The RMP framework aims to reduce the frequency and impact of any disruption to the hospital system and so its primary benefit is to avoid the incidents that may otherwise disrupt supply and cause economic loss and harm to human life.

Economic impacts of disruptions to hospital supply

Damage to critical hospital assets can generate costly immediate and longer-term impacts on the Australian economy. The immediate impacts of a disruption to hospital supply include:

- Disruption to procedures and surgeries putting patients and public safety at risk;
- Significant delays in getting treatments;
- Risk in increased mortality rates and serious conditions;
- Shortages in or destruction of essential medical supplies; and
- Lack of accessible ICU capacity and hospital beds to meet high demands

Quantifying the economic impacts associated with a disruption to the hospital system is complex. Data is relatively sparse, and the economic impacts vary as they are highly sensitive to factors including:

- Duration of the disruption; for example short disruptions are relatively manageable;
- Geographic spread of the outage, for example a localised disruption to supply means that less users are affected and substitutable goods are available (e.g. new patients are redirected to a nearby hospital); and
- Time of day/day of the week/time of the year that the outage occurs.

Computable General Equilibrium (CGE) modelling was used to illustrate how costly the incident could potentially be by examining the real-world cost of a data breach on a business in the hospital sector and an associated increase in input costs (i.e. an increase in the cost of hospital). The advantage of using a CGE approach to determine quantitative benefits is that both the direct and indirect (i.e. flow-on) economic impacts of an incident can be quantified.

CGE Modelling Approach

To analyse the direct and indirect economic contributions of an incident on a critical hospital asset in the Australian economy, a CGE approach was used to model 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 an incident on a critical hospital asset 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 data breach scenario and the rest of the economy in a framework that combines detailed historical data with fundamental economic theory.

Scenario

The CGE modelling provided estimates regarding how sensitive the Australian economy is to a shock as a result of an incident in the hospital sector. This analysis is undertaken by defining a set of hypothetical scenarios with varying magnitude of impact and resulting cost. The scope of the hypothetical scenarios is based on real-world case studies. Discussed below is the case study which informed the scope of the hypothetical scenario.

Case studies

The case study in the table below provides a basis for modelling hypothetical, but comparable incidents, in an economy-wide model and contextualising the results of that modelling. The case study was chosen to provide insights into the economy-wide costs to households and businesses of disruption events.

Incident case studies affecting critical hospital assets in Australia and globally

Incident	Summary of incident
WannaCry Cyber-attack on National Health Service (NHS)	On 12 May 2017, a cyber-attack severely disrupted over 80 hospital trusts and 8% of GP practices in the NHS, after hospitals were locked down from a ransomware cyber-attack. Hospitals and GP surgeries across England and Scotland were forced to postpone appointments. The ransomware worked by preventing users from accessing 200,000 computers via red-lettered error messages demanding Bitcoin.[380] Although the attack disrupted approximately 1% of NHS care, the Department of Health and Social Care (DHSC) report stated that the attack cost approximately £20 million ($36 million AUD) in lost output, followed by another £72 million (130 million AUD) in IT support to restore data and systems. The total cost to the NHS was £92 million (equivalent to more than $168 million AUD) due to services lost during the attack and IT costs in the aftermath.[381]

For the purposes of the modelling of the cost of avoided future incidents in Australia, the WannaCry Cyber-attack on the NHS was selected to be simulated due to the availability of sufficient information about its direct cost to support the modelling. Given the magnitude of damages associated with the incident and the size of the UK health system, this incident is considered a severe-risk scenario. The use of an actual event as a risk point of comparison is important because it ensures the benefits analysis is grounded in reality.

A framework for considering the potential impact of incidents in the Australian hospital system is provided in the table below.

Framework for scenario development and sensitivity analysis

	Severe scenario	Moderate scenario	Low scenario
Intensity of event	NHS 2017 cyber attack	50% of severe scenario	10% of severe scenario

The rationale for a less severe scenario than experienced in the NHS cyberattack incident reflects the complexity of the scenario that occurred. For an incident like the one selected for modelling,

[380] NHE 2018

[381] Ibid

the size of an organisation, existing security architecture, and time taken to detect and rectify an issue all contribute to uncertainty regarding potential cost.

While an incident with a much greater impact than the severe scenario is conceivable, the defined scenarios and subsequent benefits analysis are based on a deliberately conservative approach to ensure the severe scenario remains demonstrably plausible.

A summary of the economic impact of each scenario is provided in the table below. A break-even analysis of these benefits compared to the total estimated cost of the risk management program framework is also included in the table. This break-even analysis is expressed as the number of incidents that would need to be avoided in order for the benefits (that is, the avoided costs) of the risk management program framework to equal the costs of implementation and compliance.

Summary of benefits scenarios

	Scenario 3 (Severe), $ million	Scenario 2 (Moderate), $ million	Scenario 1 (Low), $ million
Direct avoided costs	158.0	79.0	15.8
Indirect avoided costs	71.8	35.9	7.2
Total avoided cost to the economy of the incident	229.8	114.9	23.0
Approximate number of avoided incidents per annum required for a net benefit	4.1	8.1	40.7

As noted above in the cost of option 2, the total direct ongoing cost for option 2 is expected to be $265.1 million per annum plus direct one-off costs of $342.6 million. However, the cost of the risk management program framework would also have other indirect costs flowing from increased hospital prices passed onto consumers from the framework's implementation.

After considering the economy-wide impact of this change to the cost of providing critical hospital assets, the total economic cost of the regulatory changes, including direct and indirect costs would be approximately $935.3 million per year.[382] In order for the regulatory changes to generate a net benefit, the proposed risk management program framework would need to contribute to the prevention of approximately 40 low scenario incidents every year, approximately 8 moderate scenario incidents every year, or approximately 4 severe scenario incidents every year to generate a net benefit.

It is important to note that the economic analysis of the above scenarios may not incorporate all direct avoided costs incurred by all future incidents. In the broader context of a potential future disruption, in addition to the above estimate of benefits would be the avoided costs of recovery (repair costs, costs of resulting mitigations, productivity loss due to attending to legal ramifications, intangible costs on the environment, health and wellbeing, loss of reputation, etc.).

[382]The total economic cost (being direct and indirect costs) was determined using the same CGE model approach used to estimate the benefits scenarios above. Total economic cost was determined by the CGE model and was based on an assumed economic shock equal to the cost of the draft risk management program framework (being a one-off cost of $342.6 million and an ongoing cost of $265.1 million). This resulted in a total economic impact of $935.3 million per year for the moderate scenario.

CGE modelling is a whole-of-economy approach that represents the Australian 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. In this context, indirect costs refer to flow-on costs to the economy due to supply chain linkages and other feedback responses by all economic agents (e.g. households, businesses), including those due to changes in prices or a decline in production caused by the absence of gas supply.

Further, the increasing frequency of incidents as described in section 1.1 makes the proposed risk management program framework more certain over time to exceed the anticipated costs. The examples referred to in that section demonstrate the increasing need for adequate protections against the security and resilience of critical hospital assets, and the increased likelihood that the benefits of the draft risk management program framework will exceed the costs outlined in this section.

Assessment of likely net benefit

For this particular asset class, it is more challenging to justify the benefits of regulation through economic arguments alone. The economic consequences of a disruption to hospital operation could be insignificant in comparison to the potential consequences for human life as a result of reduced, or limited access to, hospital care. Limited or reduced access to hospital can have grave consequences that can, in turn, lead to heightened risk of disease, illness or death. The estimated value of a statistical life (the value society places on reducing the risk of dying) is $5.1 million, and the value of a statistical life year (the value society places on a year of life) is $222,000.[383] As hospitals are critical to human life, any avoidance of a disruption to critical hospitals that could have otherwise increased the likelihood of disease, illness or death will have a benefit beyond that of the avoided cost to the economy able to be modelled.

The likely benefits of option 2 will be at least (and are expected to be more than) the costs of the regulation. This is primarily because, as described above and throughout this RIS, the frequency and severity of all hazard risks for critical hospital assets is growing. While some events of the magnitude described in this RIS 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, as described above, makes the proposed risk management program framework more likely to exceed the anticipated costs over time. In addition, the potential risk to human life (through illness, disease or death) is heightened in this asset class due to the criticality of hospitals to human life itself.

Further, through pursuit of option 2, the identification, mitigation and remediation of such hazards, should they occur, will be improved through:

- Lowering the material risk of hazards and subsequent impacts of those hazards, as they manifest for critical hospital assets;
- Ensuring that adoption of the risk management program framework for critical hospital assets is reasonable and proportionate to the purpose of the program;
- Avoiding regulatory duplication and facilitating a coordinated uplift in responsible entities' compliance with relevant standards; and
- Improving Government's visibility over the security and resilience of critical hospital assets.

These factors and the specific costs and benefits described above mean the likely net benefit associated with option 2 is high.

[383] Abelson, 2007

Appendix AA: Detailed costing information for critical energy market operator assets

Costing process completed by responsible entities for critical energy market operator assets

Cost submissions were received from 2 responsible entities for critical energy market operator assets.

Likely net benefit – option 2

The following section details the costs and benefits associated with option 2 (the regulatory option), before assessing the overall likely net benefit presented by this option.

Costs of option 2

There are multiple factors affecting the regulatory burden for each entity, including their existing risk management practices and capabilities, the nature of the critical energy market operator assets they operate and the size of their operations. In collecting cost information from entities across critical energy market operator assets, this variance in cost impact has been captured and reflected in the estimates of total cost across critical energy market operator assets included in this RIS.

When estimating the cost of compliance with option 2, critical energy market operator asset entities provided both an expected and a high-cost estimate. The high-cost estimate was provided as a way to measure the uncertainty associated with their estimates and the highest feasible cost of option 2. The expected estimate was used as the basis for determining the net benefit of option 2 in section 4.

Using the expected and the high estimate as a range, the cost of compliance is as follows:

- A one-off regulatory cost of between $88.3 (expected) and $230.7 million (high estimate), across critical energy market operator assets nationally; and
- An ongoing cost of between $26.9 (expected) and $57.2 million (high estimate) per year, across critical energy market operator assets nationally.

The cost of regulation will be borne by entities responsible for critical energy market operator assets who meet the relevant thresholds. Community organisations and individuals will not be directly affected but there will likely be indirect costs passed onto consumers. For the purposes of this RIS, the cost of regulation in the table below will only include the initial costs associated with regulation[384]. The indirect cost to consumers and communities has been addressed in the economic analysis through consideration of indirect cost to the wider economy as a result of the proposed RMP framework.

The average cost of compliance for each entity is estimated at $22.1 million in one-off costs and $6.7 million per year in ongoing costs, noting that there is a wide range provided in submissions from industry.

[384] Department of Prime Minister and Cabinet, 2020.

Regulatory cost estimate

Cost Type	Costs ($ million)			
	Business	Community	Individuals	Total cost ($ million)
One-off	88.3 to 230.7	Nil	Nil	88.3 to 230.7
Ongoing (per year)	26.9 to 57.2	Nil	Nil	26.9 to 57.2

Note: There will be no direct costs to individuals and communities although price rises may reflect the increased cost of operations as a result of the proposed RMP framework.

Based on the industry submissions made during consultations, total regulatory costs will be highest for rules and obligations associated with addressing cyber and information security hazards. These costs represent approximately 25.4% of the total cost of implementing the RMP framework. The cost associated with physical and natural hazards (25.0% of total costs) and general rules (22.2% of total cost) are less significant but remain material. Compliance costs associated with RMP obligations, personnel hazards, supply chain hazards and material risk rules were the least costly aspects of the RMP framework, representing in total approximately 27.4% of costs in total. The total regulatory cost by rule/obligation is set out in the table below.

Regulatory burden estimate by rule and obligation for critical energy market operator assets nationally

Rule / obligation	Costs (Expected and High)			
	One-off ($ million)	Ongoing (per year, $ million)	Total cost over 10 years ($ million) [385]	Expected estimate as percentage of total (%)
RMP obligations in SLACIP the Act	2.0 to 4.6	2.8 to 6.4	27.4 to 62.2	8.3
General rules	1.4 to 2.9	8.0 to 15.9	73.2 to 145.9	22.2
RMP rules				
Cyber and information security hazard	11.1 to 19.6	8.5 to 19.1	83.7 to 191.4	25.4
Personnel hazard	2.8 to 4.1	1.4 to 2.4	15.9 to 25.3	4.8
Supply chain hazard	1.5 to 3.0	1.4 to 2.8	15.1 to 28.3	4.6
Physical and natural hazard	67.1 to 191.6	3.7 to 8.7	102.5 to 269.6	31.1
Material risk	2.5 to 4.9	1.0 to 2.0	12.0 to 22.9	3.6
Total critical energy market operator assets	**88.3 to 230.7**	**26.9 to 57.2**	**329.7 to 745.6**	**100**

The industry submissions also indicated the type of expenditure expected to be incurred. The allocation of cost between labour effort, capital and operating costs is provided in the table below. The analysis shows that 85.0% of one-off costs and 63.3% of ongoing costs are expected to be invested in capital. A relatively small share of costs are associated with labour effort (5.2% of one-off costs and 13.6% of ongoing costs) with operating costs accounting for 9.8% of one-off costs and 23.1% of ongoing costs.

[385] For the purposes of calculating a total 10 year cost of compliance with the RMP framework, ongoing costs were assumed to commence in the year after the required implementation date (for example, for a rule requiring implementation within 2 years, the ongoing costs associated with the rule were assumed to start in year 3 of the 10 year period).

Expected one-off and ongoing costs by cost type for critical energy market operator assets nationally

Cost Type	Costs (Expected)			
	One-off ($ million)	One-off (%)	Ongoing (per year)	Ongoing (%)
Labour effort	4.6	5.2	3.7	13.6%
Capital	75.1	85.0	17.0	63.3%
Operating	8.6	9.8	6.2	23.1%
Total critical energy market operator assets	**88.3**	**100.0**	**26.9**	**100.0**

Benefits of option 2

A reliable continuous energy market operator and electricity/gas supply is central to Australia's prosperity. Further, disruption to supply can be a significant cost to the economy. The risk management program framework aims to reduce the frequency and impact of any disruption to supply and so its primary benefit is to avoid the incidents that may otherwise disrupt supply and cause economic loss.

Economic impacts of disruptions to energy market operator supply

Damage to critical energy market operator assets can subsequently disrupt the generation, transmission and/or distribution of electricity and gas to businesses and households. These events can generate costly immediate and longer-term impacts on the Australian economy. The immediate impacts of an electricity or gas outage are those associated with loss of access to electricity or increased electricity costs, such as:

- Lost production (e.g. production of goods and services may cease);
- Lost productivity (e.g. workers may be idle whilst continuing to receive wages);
- Lost wages (e.g. workers may be sent home or unable to go to work);
- Spoiled goods (e.g. spoiled produce due to lack of refrigeration); and
- Increased cost of production if switching to a substitute source of energy (e.g. backup generator).

Quantifying the economic impacts associated with the outage of energy market regulators is complex. Data is relatively sparse, and the economic impacts vary as outages are highly sensitive to factors including:

- Duration of the outage, for example short power outages are relatively manageable;
- Geographic spread of the outage, for example a localised power outage means that less users are affected and that substitutable goods (such as takeaway food) may be within travelling distance;
- Time of day/day of the week/time of the year that the outage occurs for example a power outage during business hours in the summer months will likely result in a larger economic impact than the same outage occurring in the middle of the night in winter; and
- The existence of any pre-established solutions to substitute electricity during the outage.

Computable General Equilibrium (CGE) modelling was used to illustrate how costly a disruption could potentially be by examining a hypothetical supply shock (i.e. less electricity is available to users) and an associated increase in input costs (i.e. an increase in the cost of electricity). The advantage of using a CGE approach is that both the direct and indirect (i.e. flow-on) economic impacts of a power outage event can be quantified.

CGE Modelling Approach

To analyse the direct and indirect economic contributions of power outages due to disruptions to critical infrastructure on the Australian economy, a CGE approach was used to model 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 power outages 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 outages and the rest of the economy in a framework that combines detailed historical data with fundamental economic theory.

Power outage scenarios

The CGE modelling provided estimates regarding how sensitive the Australian economy is to a shock to the electricity system. This analysis was undertaken by defining a set of hypothetical scenarios with varying magnitudes of power outages and price impacts associated with the power outage. The scope of the hypothetical scenarios was based on studies of major events which are discussed below.

Case studies

A series of case studies provides some context for how unplanned outages in the energy market operator network impact the economy. These case studies provide a basis for modelling hypothetical, but comparable outages, in an economy-wide (CGE) model and contextualising the results of that modelling. Case studies have been chosen to provide insights into the economy-wide costs to households and businesses of large-scale and severe power outages. The table below provides a summary of the case studies.

Power outage case studies in Australia and globally

Incident	Summary of incident
South Australian Blackout (2016)	On 28 September 2016, South Australia experienced a state-wide blackout. This was triggered by severe weather that damaged transmission and distribution assets, followed by reduced wind farm output and a loss of synchronism causing the loss of the Heywood Interconnector. The subsequent imbalance in supply and demand resulted in the remaining electricity generation in the state shutting down. While most supplies were restored in 8 hours, the wholesale market in South Australia was suspended for 13 days.[386]
Australia's summer bushfires threaten electricity grid (2020)	The Australian bushfires in the summer of 2020 saw unprecedented pressure on Australia's electricity grid. While the biggest potential threat, that bushfires would strike the critical interconnector linking the Victorian and New South Wales electricity grids, was not realised, accompanying extreme hot weather saw significant increases in the demand for electricity.387 The combination of catastrophic bushfires and extreme weather conditions saw some Australian customers without electricity for an extended period. The Australian Energy Market Operator (AEMO) issued a level two 'lack of reserve' warning and signalled a potential need to call on emergency power reserves to avoid widespread blackouts. Approximately 10,000 customers in the Tumbarumba and South Coast regions, as well as

[386] Australian Energy Regulator, 2018.

[387] Foley 2020

Incident	Summary of incident
	an additional 5,800 were without electricity between New Years Eve of 2019 and early January 2020.[388]

While this RIS seeks to leverage the examples outlined above, it does not mean that a single, equivalent event is needed for costs and benefits to break-even. The chosen examples are intended to be demonstrative of potential costs only, rather than the specific events which may lead to disruption. It may be the case that a series of smaller, less significant disruptions occur over the course of a year and accumulate to result in disruption of a similar scale.

The above case studies highlight that widespread power outages inflict substantial direct and indirect costs on firms and households alike. Businesses bore the brunt of the damage across all these case studies, mostly through lost income and productivity.

For the purposes of the modelling of the cost of avoided future incidents in Australia, the South Australian blackout of 2016 was used as the baseline (moderate) risk scenario. The use of an actual event as the baseline risk point of comparison is important because it ensures the benefits analysis is grounded in reality. The scale of the event is not theoretical and there is sufficient information about the event to support modelling. The 2016 South Australian blackout was estimated to have approximately 5-8 GWh of unserved energy (electricity that would otherwise have been used by customers but that was not available because of the supply interruption).389 Further, while an event of this magnitude has previously been considered to represent the worst-case power outage incident in Australia, the increasing severity and frequency of similar incidents detailed in section 1.1, particularly in the context of growing all hazards incidents, represents a risk to the whole economy.

A framework for considering the potential impacts of Australian power outages following failure of critical infrastructure is provided in the table below.

Framework for scenario development and sensitivity analysis

	Severe scenario	Moderate scenario	Low scenario
Intensity of event	150% of moderate scenario costs	South Australian 2016 Blackout	50% of moderate scenario costs

The rationale for a more severe scenario than experienced in South Australia reflects the complexity of the scenarios that could occur. As noted above, the economic impact of an incident will vary due to a range of factors including the location of a disruption, the month and time of day at which the disruption occurs, the day of the week on which the disruption takes place and the duration of disruption. Accounting for an incident that has a greater economic impact than the South Australian blackout is necessary to reflect the possibility that a disruption of the same scale (in terms of unserved energy) could impact areas where there would be greater economic impact than in South Australia in September at 4 pm. While an incident with a much greater impact than the severe scenario is conceivable (for example, a cyber-caused outage could be highly disruptive, by impacting a number of critical assets in the grid simultaneously), the defined scenarios and subsequent benefits analysis has taken a deliberately conservative approach to ensure the severe scenario remains demonstrably plausible.

A summary of the economic impact of each scenario is provided in the table below. Direct avoided costs refer to the financial costs directly incurred as a result of an incident, while indirect costs refer to flow-on costs to the economy due to supply chain linkages and other feedback responses by all

[388] Ibid

[389] AEMO, 2018, Australian Energy Regulator, 2020; AEMC, 2019

economic agents (e.g., households, businesses). A break-even analysis of these benefits compared to the total estimated cost of the risk management program framework is also included in the table. This break-even analysis is expressed as the number of incidents that would need to be avoided in order for the benefits (that is, the avoided costs) of the risk management program framework to equal the costs of implementation and compliance.

Summary of benefits scenarios

	Scenario 1 (Severe), $ million	Scenario 2 (Moderate), $ million	Scenario 3 (Low), $ million
Direct avoided cost	585.0	390.0 (a)	195.0
Indirect avoided costs	695.0 (b)	460.0 (b)	295.0(b)
Total avoided cost to the economy of the incident	1,280.0	850.0	490.0
Approximate number of avoided incidents per annum required for a net benefit	Less than 0.1	Less than 0.1	0.1

Notes:
(a) According to Blackout Survey Results by Business South Australia (2016), total costs to South Australian businesses reached $390 million (inflated into 2020 Australian dollars) as a result of the power outage.
(b) In response to the 2016 blackout, the South Australian government installed a Tesla battery to improve their resilience to future events. As a result, indirect costs include the capital cost for installing the battery ($90 million) and costs for provision of network services ($4 million per year over 10 years).

As noted above, the total direct ongoing cost for option 2 is expected to be $26.9 million per annum plus direct one-off costs of $88.3 million. However, the cost of the risk management program framework would also have other indirect costs flowing from increased energy prices passed onto consumers from the framework's implementation.

After considering the economy-wide impact of this change to the cost of providing electricity and/or gas, the total economic cost of the regulatory changes, including direct and indirect costs would be approximately $68.6 million per year.[390] In order for the regulatory changes to generate a net benefit, the proposed risk management program framework would need to contribute to the prevention of approximately 1 low scenario incident every 7 years, 1 moderate scenario incident every 12.5 years or 1 severe scenario every 20 years to generate a net benefit.

It is important to note that the economic analysis of the above scenarios does not incorporate all direct avoided costs incurred by all future incidents. The avoided costs included are only those which were directly and immediately incurred as a result of the South Australian incident. In the broader context of a potential future disruption, in addition to the above estimate of benefits would be the avoided costs of recovery (repair costs, costs of resulting mitigations) from high value, specific circumstances which were not experienced during the South Australian blackout.

Further, the increasing frequency of incidents as described in section 1.1 makes the proposed risk management program framework more certain over time to exceed the anticipated costs. The

[390]The total economic cost (being direct and indirect costs) was determined using the same CGE model approach used to estimate the benefits scenarios above. Total economic cost was determined by the CGE model and was based on an assumed economic shock equal to the cost of the draft risk management program framework (being a one-off cost of $88.3 million and an ongoing cost of $26.9 million). This resulted in a total economic impact of $68.6 million per year for the moderate scenario.

CGE modelling is a whole-of-economy approach that represents the Australian 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. In this context, indirect costs refer to flow-on costs to the economy due to supply chain linkages and other feedback responses by all economic agents (e.g. households, businesses), including those due to changes in prices or a decline in production caused by the absence of electricity supply.

examples referred to in that section demonstrate the increasing need for adequate protections against the security and resilience of critical energy market operator assets, and the increased likelihood that the benefits of the draft risk management program framework will exceed the costs outlined in this section.

Assessment of likely net benefit

The likely benefits of option 2 will be at least (and are expected to be more than) the costs of the regulation. This is primarily because, as described above and throughout this RIS, the frequency and severity of all hazard risks for critical energy market operator assets are growing. While some events of the magnitude described in this RIS 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, as described above, makes the proposed risk management program framework more likely to exceed the anticipated costs over time.

Further, through pursuit of option 2, the identification, mitigation and remediation of such hazards, should they occur, will be improved through:

- Lowering the material risk of hazards and subsequent impacts of those hazards, as they manifest for critical energy market operator assets;
- Ensuring that adoption of the risk management program framework for critical energy market operator assets is reasonable and proportionate to the purpose of the program;
- Avoiding regulatory duplication and facilitating a coordinated uplift in responsible entities' compliance with relevant standards; and
- Improving Government's visibility over the security and resilience of critical energy market operator assets.

Overall, these factors and the specific costs and benefits described above mean the likely net benefit associated with option 2 is high.

Appendix BB: Detailed costing information for critical freight infrastructure and critical freight services assets

Costing process completed by responsible entities for critical freight infrastructure and critical freight services assets

Cost submissions were received from 5 responsible entities for critical freight infrastructure and critical freight services assets. This represented approximately 32.2% of the total critical freight infrastructure and critical freight services asset market.

Likely net benefit – option 2

The following section details the costs and benefits associated with option 2 (the regulatory option), before assessing the overall likely net benefit presented by this option.

Costs of option 2

There are multiple factors affecting the regulatory burden for each entity, including their existing risk management practices and capabilities, the nature of the critical freight infrastructure and critical freight services they operate and the size of their operations. In collecting cost information from entities across critical freight infrastructure and critical freight services, this variance in cost impact has been captured and reflected in the estimates of total cost across critical freight infrastructure and critical freight services assets included in this RIS.

When estimating the cost of compliance with option 2, critical freight infrastructure and critical freight services asset entities provided both an expected and a high-cost estimate. The high-cost estimate was provided as a way to measure the uncertainty associated with their estimates and the highest feasible cost of option 2. The expected estimate was used as the basis for determining the net benefit of option 2 in section 4.

Using the expected and the high estimate as a range, the cost of compliance is as follows:

- A one-off regulatory cost of between $60.9 (expected) and $163.9 million (high estimate), across critical freight infrastructure and critical freight services assets nationally; and
- An ongoing cost of between $50.0 (expected) and $71.0 million (high estimate) per year, across critical freight infrastructure and critical freight services assets nationally.

The average cost of compliance for each entity is estimated at $2.3 million in ongoing costs and $3.9 million per year in one-off costs.

The cost of regulation will be borne by entities responsible for critical freight infrastructure and critical freight services who meet the relevant thresholds. Community organisations and individuals will not be directly affected but there will likely be indirect costs passed onto consumers. For the purposes of this RIS, the cost of regulation in the table below will only include the initial costs associated with regulation.[391] The indirect cost to consumers and communities has been addressed in the economic analysis through consideration of indirect cost to the wider economy as a result of the proposed RMP framework.

[391] Department of Prime Minister and Cabinet, 2020

Regulatory cost estimate

Cost Type	Costs ($ million)			
	Business	Community	Individuals	Total cost
One-off	60.9 to 163.9	Nil	Nil	60.9 to 163.9
Ongoing (per year)	50.0 to 71.0	Nil	Nil	50.0 to 71.0

Note: There will be no direct costs to individuals and communities although price rises may reflect the increased cost of operations as a result of the proposed RMP framework.

Based on the industry submissions made during consultations, total regulatory costs will be highest for rules and obligations associated with addressing risk RMP obligations in the Act. These costs represent approximately 27.4% of the total cost of implementing the RMP framework. The cost associated with supply chain hazards (22.8% of total cost), cyber and information security hazards (16.9% of total cost) and material risk rules (12.5% of total cost) are less significant but remain material. Compliance costs associated with general rules, personnel hazards and physical and natural hazards were the least costly aspects of the RMP framework, representing in total approximately 20.4% of costs in total. The total regulatory cost by rule/obligation is set out in the table below.

Regulatory burden estimate by rule and obligation for critical freight infrastructure and critical freight services nationally

Rule / obligation	Costs (Expected and High)			
	One-off ($ million)	Ongoing (per year, $ million)	Total cost over 10 years ($ million) [392]	Expected estimate as a percentage of total (%)
RMP obligations in the Act	13.4 to 103.2	14.6 to 33.5	144.7 to 404.7	27.4
General rules	4.3 to 22.8	1.4 to 2.2	16.5 to 42.3	3.1
RMP Rules				
Cyber and information security hazard	9.3 to 6.1	8.4 to 4.7	89.2 to 50.9	16.9
Personnel hazard	4.2 to 8.7	3.3 to 5.9	35.9 to 64.4	6.8
Supply chain hazard	9.1 to 5.6	11.7 to 12.2	120.5 to 121.6	22.8
Physical and natural hazard	6.3 to 6.1	5.2 to 7.3	55.2 to 75.0	10.5
Material risk	14.3 to 11.4	5.4 to 5.3	65.8 to 61.9	12.5
Total critical freight infrastructure and critical freight services assets	**60.9 to 163.9**	**50.0 to 71.0**	**527.8 to 820.7**	**100**

The industry submissions also indicated the type of expenditure expected to be incurred. The allocation of expected cost between labour effort, capital and operating costs is provided in the

[392] For the purposes of calculating a total 10 year cost of compliance with the RMP framework, ongoing costs were assumed to commence in the year after the required implementation date (for example, for a rule requiring implementation within 2 years, the ongoing costs associated with the rule were assumed to start in year 3 of the 10 year period).

table below. The analysis shows that 43.8% of one-off costs and 35.8% of ongoing costs are expected to be invested in capital. A relatively small share of costs is associated with labour effort for one-off and ongoing costs (18.6% for one-off costs and 20.1% for ongoing costs). Operating costs are the largest component of ongoing costs (44.1% of total ongoing costs) and account for 37.6% of one-off costs.

Expected one-off and ongoing costs by cost type for critical freight infrastructure and critical freight services assets nationally

Cost Type	Costs			
	One-off ($ million)	One-off (%)	Ongoing (per year)	Ongoing (%)
Labour effort	11.3	18.6%	10.1	20.1%
Capital	26.7	43.8%	17.9	35.8%
Operating	22.9	37.6%	22.1	44.1%
Total critical freight infrastructure and critical freight services assets	**60.9**	**100%**	**50.0**	**100.0%**

Benefits of option 2

A reliable and resilient freight infrastructure and services network is central to Australia's prosperity. Further, disruption to its operation can lead to significant cost and impact on the economy. The RMP framework aims to reduce the frequency and impact of any disruption to supply and so its primary benefit is to avoid the incidents that may otherwise disrupt supply and cause economic loss.

Economic impacts of disruptions to freight infrastructure and freight services

Disruption of freight infrastructure and freight services, which form crucial parts of the supply chain for Australian imports, exports, and domestic consumption, can affect businesses and households alike. Such disruptions can have costly immediate and longer-term impacts on the economy. The immediate impacts of a disruption to freight infrastructure and freight services are those associated with reduced capacity and increased costs, such as:

- Reduced economic activity (e.g. disrupted movement of consumer goods and subsequent impacts on business);
- Lost productivity as a result of reduced economic activity (e.g. workers may be idle whilst continuing to receive wages);
- Lost wages (e.g. workers may be sent home or unable to go to work); and
- Spoiled goods (e.g. perishable goods may be unsuitable for sale or consumption due to delayed caused by reduced freight capacity).

Computable General Equilibrium (CGE) modelling was used to illustrate how costly the disruption could potentially be by examining a hypothetical shock (i.e. reduced freight capacity) and an associated increase in input costs (i.e. an increase in the cost of freight infrastructure or services). The advantage of using a CGE approach is that both the direct and indirect (i.e. flow-on) economic impacts of a power outage event can be quantified.

CGE Modelling Approach

To analyse the direct and indirect economic contributions of a freight disruption due to disruptions to critical infrastructure on the Australian economy, a CGE approach was used to model 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 a freight disruption 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 outage and the rest of the economy in a framework that combines detailed historical data with fundamental economic theory.

Scenarios

The CGE modelling provided estimates regarding how sensitive the Australian economy is to a shock to the freight system. This analysis was undertaken by deriving a set of hypothetical modelling scenarios based on assumptions about the impact of a disruption to freight infrastructure or services. The scope of the hypothetical scenarios was based on studies of major events which are discussed below.

Case studies

The case studies provided in the table below provide a basis for modelling hypothetical, but comparable outages, in an economy-wide model and contextualising the results of that modelling. Case studies have been chosen to provide insights into the economy-wide costs to households and businesses of large-scale and severe freight disruption events.

Freight disruption case studies

Incident	Summary of incident
TNT Express targeted in NotPeyta attack (2017)	FedEx subsidiary company TNT Express fell victim to 'NotPeyta' ransomware and malware attacks in 2017. The cyber-attack disrupted computer systems and IT operations which caused deliveries and sales to suffer in all countries of operation, including Australia. FedEx reported that the attack cost TNT Express approximately USD300.0 million (AUD 416.7 million) in lost earnings due to disrupted operations, loss of systems and extended recovery times.
ForwardAir ransomware attack (2020)	ForwardAir, a trucking company operating in the United States and Canada, was hit by a 'Hades' ransomware attack in December 2020. The incident impacted operational and information technology systems and included a data breach. The company suspended all electronic customer databases temporarily to limit the impact of the attack. The attack cost approximately USD 7.5 million (AUD 10.4 million) in less than load freight revenue.

These case studies highlight that disruptions to critical freight assets can inflict substantial direct and indirect costs on firms and households alike. The TNT express attack had widespread impacts across the globe, affecting deliveries and sales. The ForwardAir attack, while smaller in scale and cost, had similarly widespread impacts, with employees unable to access documentation to transport goods through customs.

For the purposes of the modelling of the cost of avoided future incidents in Australia, both case studies were used as baseline scenarios. The TNT Express attack was used as the severe baseline, and the ForwardAir attack as the low baseline. The use of actual events as baseline risk points of comparison is important because it ensures the benefits analysis is grounded in reality.

The scale of the event is not theoretical and there is sufficient information about the event to support modelling.

A framework for considering the potential impacts of the freight disruption following failure of critical infrastructure is provided in the table below.

Framework for scenario development and sensitivity analysis

	Severe scenario	Moderate scenario	Low scenario
Intensity of event	TNT Express NotPeyta attack (2017)	50% of severe scenario	ForwardAir ransomware attack (2020)

The rationale for a range of scenarios reflects the complexity of the scenarios that could occur. As noted above, the economic impact of an incident will vary due to a range of factors including the location of a disruption, the month and time of day at which the disruption occurs, the day of the week on which the disruption takes place and the duration of disruption. For example, accounting for an incident that has a greater economic impact than the ForwardAir ransomware attack is necessary to reflect the possibility that a disruption of a similar scale could impact areas where there would be greater economic impact than in that incident. Similarly, the TNT Express incident affected a subsidiary of one of the world's largest freight companies, and a similar incident that affected a smaller operator would have a plausibly reduced impact. While an incident with a much greater impact than the severe scenario is conceivable, the defined scenarios and subsequent benefits analysis has taken a deliberately conservative approach to ensure the severe scenario remains demonstrably plausible.

A summary of the economic impact of each scenario is provided in the table below. Direct avoided costs refer to the financial costs directly incurred as a result of an incident, while indirect costs refer to flow-on costs to the economy due to supply chain linkages and other feedback responses by all economic agents (e.g., households, businesses). A break-even analysis of these benefits compared to the total estimated cost of the risk management program framework is also included in the table. This break-even analysis is expressed as the number of incidents that would need to be avoided in order for the benefits (that is, the avoided costs) of the risk management program framework to equal the costs of implementation and compliance.

Summary of benefits scenarios

	Scenario 1 (Severe), $ million	Scenario 2 (Moderate), $ million	Scenario 3 (Low), $ million
Direct avoided cost	416.7	208.3	10.4
Indirect avoided costs	307.5	153.7	7.7
Total avoided cost to the economy of the incident	724.1	362.0	18.1
Approximate number of avoided incidents per annum required for a net benefit	Approximately 0.4 incidents every year	Approximately 0.8 incidents per year	Approximately 15.6 incidents every year

As noted above, the total direct ongoing cost for option 2 is expected to be $50.0 million per annum plus direct one-off costs of $60.9 million. However, the cost of the risk management program framework would also have other indirect costs flowing from increased freight prices passed onto consumers from the framework's implementation.

After considering the economy-wide impact of this change to the cost of providing freight, the total economic cost of the regulatory changes, including direct and indirect costs would be approximately $281.6 million per year.[393] In order for the regulatory changes to generate a net benefit, the proposed risk management program framework would need to contribute to the prevention of approximately 0.4 severe scenario incidents every year, 0.8 moderate scenario incidents every year or 18.1 low scenario incidents every year to generate a net benefit.

It is important to note that the economic analysis of the above scenarios does not incorporate all direct avoided costs incurred by all future incidents. The avoided costs included are only those which were directly and immediately incurred as a result of the incidents modelled. In the broader context of a potential future disruption, in addition to the above estimate of benefits would be the avoided costs of recovery (repair costs, costs of resulting mitigations) from high value, specific circumstances which were not experienced during the modelled incidents.

Further, the increasing frequency of incidents as described in section 1.1 makes the proposed risk management program framework more certain over time to exceed the anticipated costs. The examples referred to in that section demonstrate the increasing need for adequate protections against the security and resilience of critical freight infrastructure and freight services assets, and the increased likelihood that the benefits of the draft risk management program framework will exceed the costs outlined in this section.

[393]The total economic cost (being direct and indirect costs) was determined using the same CGE model approach used to estimate the benefits scenarios above. Total economic cost was determined by the CGE model based on an assumed economic shock equal to the cost of the draft risk management program framework (being a one-off cost of $60.9 million and an ongoing cost of $50.0 million). This was a total economic impact of $281.6 million per year for the moderate scenario.

CGE modelling is a whole-of-economy approach that represents the Australian 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. In this context, indirect costs refer to flow-on costs to the economy due to supply chain linkages and other feedback responses by all economic agents (e.g. households, businesses), including those due to changes in prices or a decline in production caused by the absence of freight supply.

Assessment of likely net benefit

The likely benefits of option 2 will be at least (and are expected to be more than) the costs of the regulation. This is primarily because, as described above and throughout this RIS, the frequency and severity of all hazard risks for critical freight infrastructure and freight services assets are growing. While some events of the magnitude described in this RIS 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, as described above, makes the proposed risk management program framework more likely to exceed the anticipated costs over time.

Further, through pursuit of option 2, the identification, mitigation and remediation of such hazards, should they occur, will be improved through:

- Lowering the material risk of hazards and subsequent impacts of those hazards, as they manifest for critical freight infrastructure and freight services assets;
- Ensuring that adoption of the risk management program framework for critical freight infrastructure and freight services assets is reasonable and proportionate to the purpose of the program;
- Avoiding regulatory duplication and facilitating a coordinated uplift in responsible entities' compliance with relevant standards; and
- Improving Government's visibility over the security and resilience of critical freight infrastructure and freight services assets.

Overall, these factors and the specific costs and benefits described above mean the likely net benefit associated with option 2 is high.

Appendix CC: Detailed costing information for critical food and grocery assets

Costing process completed by responsible entities for critical food and grocery assets

Cost submissions were received from three responsible entities for critical food and grocery assets. This represented approximately 74.5% of the total critical food and grocery asset market.

Likely net benefit – option 2

The following section details the costs and benefits associated with option 2 (the regulatory option), before assessing the overall likely net benefit presented by this option.

Costs of option 2

There are multiple factors affecting the regulatory burden for each entity, including their existing risk management practices and capabilities, the nature of the critical food and grocery service they operate and the size of their operations. In collecting cost information from entities across critical food and grocery assets, this variance in cost impact has been captured and reflected in the estimates of total cost across critical food and grocery assets included in this RIS.

When estimating the cost of compliance with option 2, critical food and grocery asset entities provided both an expected and a high-cost estimate. The high-cost estimate was provided as a way to measure the uncertainty associated with their estimates and the highest feasible cost of option 2. The expected estimate was used as the basis for determining the net benefit of option 2 in section 4.

Using the expected and the high estimate as a range, the cost of compliance is as follows:

- A one-off regulatory cost of between $12.2 (expected) and 28.2 million (high estimate), across critical food and grocery assets nationally; and
- An ongoing cost of between $6.6 (expected) and $15.6 million (high estimate) per year, across critical food and grocery assets nationally.

The average cost of compliance for each entity is estimated at $3.1 million in one-off costs and $1.7 million per year in ongoing costs.

The cost of regulation will be borne by entities responsible for critical food and grocery who meet the relevant thresholds. Community organisations and individuals will not be directly affected but there will likely be indirect costs passed onto consumers. For the purposes of this RIS, the cost of regulation in the table below will only include the initial costs associated with regulation.[394] The indirect cost to consumers and communities has been addressed in the economic analysis through consideration of indirect cost to the wider economy as a result of the proposed RMP framework.

Regulatory cost estimate

Cost Type	Costs ($ million)			
	Business	Community	Individuals	Total cost

[394] Department of Prime Minister and Cabinet, 2020

One-off	12.2 to 28.2	Nil	Nil	12.2 to 28.2
Ongoing (per year)	6.6 to 15.6	Nil	Nil	6.6 to 15.6

Note: There will be no direct costs to individuals and communities although price rises may reflect the increased cost of operations as a result of the proposed RMP framework.

Based on the industry submissions made during consultations, total regulatory costs will be highest for rules and obligations associated with addressing cyber and information security hazards. These costs represent approximately 42.6% of the total cost of implementing the RMP framework. The cost associated with physical and natural hazards (12.9% of total cost), personnel hazards (12.6% of total cost) and supply chain hazards (12.0% of total cost) are less significant but remain material. The total regulatory cost by rule/obligation is set out in the table below.

Regulatory burden estimate by rule and obligation for critical food and grocery assets nationally

Rule / obligation	Costs (Expected and High)			
	One-off ($ million)	Ongoing (per year, $ million)	Total cost over 10 years ($ million) [395]	Expected estimate as a percentage of total (%)
RMP obligations in the Act	1.0 to 2.1	0.3 to 0.5	3.7 to 6.5	5.1
General rules	1.1 to 2.0	0.2 to 0.4	3.1 to 6.0	4.3
RMP Rules				
Cyber and information security hazard	3.9 to 9.6	3.1 to 7.5	31.0 to 75.3	42.6
Personnel hazard	1.0 to 1.8	0.9 to 1.4	9.2 to 15.3	12.6
Supply chain hazard	1.6 to 4.3	0.8 to 2.2	8.8 to 25.1	12.0
Physical and natural hazard	2.2 to 4.4	0.8 to 1.5	9.4 to 18.8	12.9
Material risk	1.3 to 4.0	0.7 to 2.0	7.7 to 23.1	10.6
Total critical food and grocery assets	**12.2 to 28.2**	**6.6 to 15.6**	**72.9 to 170.0**	**100**

The industry submissions also indicated the type of expenditure expected to be incurred. The allocation of expected cost between labour effort, capital and operating costs is provided in the table below. The analysis shows that 44.5% of one-off costs and 36.4% of ongoing costs are expected to be invested in capital. A relatively small share of costs is associated with labour effort for one-off and ongoing costs (17.3% for one-off costs and 38.2% for ongoing costs). Operating costs are the largest component of ongoing costs (44.9% of total ongoing costs) and account for 38.2% of one-off costs.

Expected one-off and ongoing costs by cost type for critical food and grocery assets nationally

Cost Type	Costs			
	One-off ($	One-off	Ongoing	Ongoing

[395] For the purposes of calculating a total 10 year cost of compliance with the RMP framework, ongoing costs were assumed to commence in the year after the required implementation date (for example, for a rule requiring implementation within 2 years, the ongoing costs associated with the rule were assumed to start in year 3 of the 10 year period).

	million)	(%)	(per year)	(%)
Labour effort	2.7	22.3	2.0	29.8
Capital	4.7	38.3	0.7	10.0
Operating	4.8	39.4	4.0	60.2
Total critical food and grocery assets	**12.2**	**100**	**6.6**	**100.0**

Benefits of option 2

A reliable and resilient food and grocery infrastructure and services network is central to Australia's prosperity. Further, disruption to its operation can lead to significant cost and impact on the economy. The RMP framework aims to reduce the frequency and impact of any disruption to supply and so its primary benefit is to avoid the incidents that may otherwise disrupt supply and cause economic loss.

Economic impacts of disruptions to food and grocery services

Disruption of food and grocery services, which form crucial parts of the supply chain for Australian imports, exports, and domestic consumption, can affect businesses and households alike. Such disruptions can have costly immediate and longer-term impacts on the economy. The immediate impacts of a disruption to food and grocery services are those associated with reduced capacity and increased costs, such as:

- Reduced economic activity (e.g. disrupted movement of consumer goods and subsequent impacts on business);
- Lost productivity as a result of reduced economic activity (e.g. workers may be idle whilst continuing to receive wages);
- Lost wages (e.g. workers may be sent home or unable to go to work); and
- Spoiled goods (e.g. perishable goods may be unsuitable for sale or consumption due to delayed caused by reduced food and grocery capacity).

Computable General Equilibrium (CGE) modelling was used to illustrate how costly the disruption could potentially be by examining a hypothetical shock (i.e. reduced food and grocery capacity) and an associated increase in input costs (i.e. an increase in the cost of food and grocery infrastructure or services). The advantage of using a CGE approach is that both the direct and indirect (i.e. flow-on) economic impacts of a power outage event can be quantified.

CGE Modelling Approach

To analyse the direct and indirect economic contributions of a food and grocery disruption due to disruptions to critical infrastructure on the Australian economy, a CGE approach was used to model 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 a food and grocery disruption 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 outage and the rest of the economy in a framework that combines detailed historical data with fundamental economic theory.

Scenarios

The CGE modelling provided estimates regarding how sensitive the Australian economy is to a shock to the food and grocery system. This analysis was undertaken by deriving a set of hypothetical modelling scenarios based on assumptions about the impact of a disruption to food and grocery infrastructure or services. The scope of the hypothetical scenarios was based on studies of major events which are discussed below.

Case studies

The case studies provided in the table below provide a basis for modelling hypothetical, but comparable outages, in an economy-wide model and contextualising the results of that modelling. Case studies have been chosen to provide insights into the economy-wide costs to households and businesses of large-scale and severe food and grocery disruption events.

Food and grocery disruption case studies

Incident	Summary of incident
Coop Supermarket closures (2021)	In 2021, more than half of all Coop Supermarkets in Sweden were forced to close for nearly a week as the result of a cyber-attack. Around 500 supermarkets were closed for nearly a week, reducing consumer access and choice for fresh food and grocery produce. Kaseya announced it had received a universal decryptor tool for the REvil-encrypted files from an unnamed "trusted third party" and was helping victims restore their files. It is suggested that the cost of this breach and consequent closure of stores cost Coop AUD$28 million.[396]
JBS meat processing ransomware attack (2021)	JBS Foods Group, is the world's largest meat processing company, supplying one-fifth of meat globally, with a global footprint including Australia. JBS US Headquarters was the target of an organised cybersecurity attack, affecting some of the servers supporting its North American and Australian IT systems. JBS Foods Group closed all of its beef processing plants in the US, Canada and Australia, resulting in over 7000 employees being temporarily stood down in Australia alone. JBS Food Groups paid the equivalent of $US11 million ($14.2 million) to a criminal gang to end a five-day cyber attack.[397]

These case studies highlight that disruptions to critical food and grocery assets can inflict substantial direct and indirect costs on firms and households alike. The Coop supermarket attack had widespread impacts on the community during the closure periods, affecting sales and the ability of the community to access food and groceries. The JBS attack had impacts across the globe, affecting deliveries, sales and meat prices.

For the purposes of the modelling of the cost of avoided future incidents in Australia, both case studies were used as baseline scenarios. The Coop Supermarket attack was used as the moderate baseline, and the JBS attack as the low baseline. The use of actual events as baseline risk points of comparison is important because it ensures the benefits analysis is grounded in reality. The scale of the event is not theoretical and there is sufficient information about the event to support modelling.

[396] https://www.statista.com/statistics/1063165/revenue-of-coop-retail-stores-in-sweden-by-region/

[397] https://www.abc.net.au/news/rural/2021-06-10/jbs-foods-pays-14million-ransom-cyber-attack/100204240

A framework for considering the potential impacts of the food and grocery disruption following failure of critical infrastructure is provided in the table below.

Framework for scenario development and sensitivity analysis

	Severe scenario	Moderate scenario	Low scenario
Intensity of event	150% of Moderate scenario	Coop Supermarket attack (2021)	JBS attack (2021)

The rationale for a range of scenarios reflects the complexity of the scenarios that could occur. As noted above, the economic impact of an incident will vary due to a range of factors including the location of a disruption, the month and time of day at which the disruption occurs, the day of the week on which the disruption takes place and the duration of disruption. For example, accounting for an incident that has a greater economic impact than the Coop Supermarket ransomware attack is necessary to reflect the possibility that a disruption of a similar scale could impact areas where there would be greater economic impact than in that incident. While an incident with a much greater impact than the severe scenario is conceivable, the defined scenarios and subsequent benefits analysis has taken a deliberately conservative approach to ensure the severe scenario remains demonstrably plausible.

A summary of the economic impact of each scenario is provided in the table below. Direct avoided costs refer to the financial costs directly incurred as a result of an incident, while indirect costs refer to flow-on costs to the economy due to supply chain linkages and other feedback responses by all economic agents (e.g., households, businesses). A break-even analysis of these benefits compared to the total estimated cost of the risk management program framework is also included in the table. This break-even analysis is expressed as the number of incidents that would need to be avoided in order for the benefits (that is, the avoided costs) of the risk management program framework to equal the costs of implementation and compliance.

Summary of benefits scenarios

	Scenario 1 (Severe), $ million	Scenario 2 (Moderate), $ million	Scenario 3 (Low), $ million
Direct avoided cost	42.0	28.0	14.2
Indirect avoided costs	30.0	20.0	10.1
Total avoided cost to the economy of the incident	72.0	48.0	24.3
Approximate number of avoided incidents per annum required for a net benefit	Less than 0.2 incidents every year	Less than 0.3 incidents per year	Approximately 0.5 incidents every year

As noted above, the total direct ongoing cost for option 2 is expected to be $6.6 million per annum plus direct one-off costs of $12.2 million. However, the cost of the risk management program framework would also have other indirect costs flowing from increased food and grocery prices passed onto consumers from the framework's implementation.

After considering the economy-wide impact of this change to the cost of providing food and groceries, the total economic cost of the regulatory changes, including direct and indirect costs would be approximately $12.5 million per year.[398] In order for the regulatory changes to generate a net benefit, the proposed risk management program framework would need to contribute to the prevention of approximately 0.2 severe scenario incidents every year, 0.3 moderate scenario incidents every year or 0.5 low scenario incidents every year to generate a net benefit.

It is important to note that the economic analysis of the above scenarios does not incorporate all direct avoided costs incurred by all future incidents. The avoided costs included are only those which were directly and immediately incurred as a result of the incidents modelled. In the broader context of a potential future disruption, in addition to the above estimate of benefits would be the avoided costs of recovery (repair costs, costs of resulting mitigations) from high value, specific circumstances which were not experienced during the modelled incidents.

Further, the increasing frequency of incidents as described in section 1.1 makes the proposed risk management program framework more certain over time to exceed the anticipated costs. The examples referred to in that section demonstrate the increasing need for adequate protections against the security and resilience of critical food and grocery services assets, and the increased likelihood that the benefits of the draft risk management program framework will exceed the costs outlined in this section.

[398]The total economic cost (being direct and indirect costs) was determined using the same CGE model approach used to estimate the benefits scenarios above. Total economic cost was determined by the CGE model based on an assumed economic shock equal to the cost of the draft risk management program framework (being a one-off cost of $12.2 million and an ongoing cost of $6.6 million). This was a total economic impact of $12.5 million per year for the moderate scenario.

CGE modelling is a whole-of-economy approach that represents the Australian 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. In this context, indirect costs refer to flow-on costs to the economy due to supply chain linkages and other feedback responses by all economic agents (e.g. households, businesses), including those due to changes in prices or a decline in production caused by the absence of freight supply.

Assessment of likely net benefit

The likely benefits of option 2 will be at least (and are expected to be more than) the costs of the regulation. This is primarily because, as described above and throughout this RIS, the frequency and severity of all hazard risks for critical food and grocery assets are growing. While some events of the magnitude described in this RIS 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, as described above, makes the proposed risk management program framework more likely to exceed the anticipated costs over time.

Further, through pursuit of option 2, the identification, mitigation and remediation of such hazards, should they occur, will be improved through:

- Lowering the material risk of hazards and subsequent impacts of those hazards, as they manifest for critical food and grocery assets;
- Ensuring that adoption of the risk management program framework for critical food and grocery assets is reasonable and proportionate to the purpose of the program;
- Avoiding regulatory duplication and facilitating a coordinated uplift in responsible entities' compliance with relevant standards; and
- Improving Government's visibility over the security and resilience of critical food and grocery assets.

Overall, these factors and the specific costs and benefits described above mean the likely net benefit associated with option 2 is high.