Supplementary analysis for Critical Telecommunications Assets

Overview of the role of telecommunications in Australia

Telecommunications assets are central to social and economic activity in Australia.[1] Industry, government and individuals make daily use of services enabled by telecommunications networks and related assets, which involve the electronic transmission of data and information between users. Telecommunications assets are relied on and share interdependencies with all critical infrastructure sectors and are particularly important to:

- banking and finance;
- healthcare;
- logistics;
- energy transmission; and
- government and defence activities, including disaster responses.

The COVID-19 pandemic and an increasing occurrence of significant natural disasters have reaffirmed the importance of reliable telecommunications assets. Disruptions, including by sabotage, causes significant impacts on reliant critical services and end-users. Further, telecommunications assets store and transmit highly sensitive Australian data, making them a primary target for espionage activities.

Impacts of a disruption to telecommunications assets

Disruptions to telecommunications assets can cause a wide array of consequences, including:

- In the case of **natural disasters,** which typically damage above-ground network components and energy supply, public safety risks may arise if:
    - the public are unable to receive emergency warnings via national warning systems;
    - telecommunications networks are overloaded, making it difficult for essential calls to be connected; or
    - there are delays in restoring telecommunications assets, where telecommunications carriers have to wait for safe conditions to repair systems or provide temporary telecommunications facilities.
- The realisation of other **physical risks** may result in the reduced or suspended operation of a telecommunications asset. Outages may be nation-wide and include:
    - outages to payment systems;
    - no access to emergency services;
    - downstream asset outages if they rely on data storage or cloud services to function; and
    - disrupted supply chains, including in freight and food and grocery sectors.
- Where a **cyber-attack** occurs, telecommunications assets holding sensitive data may be compromised. Where an asset also maintains cloud and data services for corporate customers, a cyber-attack may allow access to these corporations' systems and consequently, compromise of their commercial or customer data. A cyber-attack may also allow hostile adversaries access to

[1] Australian Infrastructure Audit 2019 - 8. Telecommunications.pdf, pg556, infrastructure.gov.au/Australia-infrastructure-audit.

sensitive law-enforcement and intelligence related data, including interception capability plans prepared in compliance with the *Telecommunications (Interception and Access) Act 1979*.

- With **complex supply chains** and increasing integration between international networks, software and hardware, telecommunications assets are experiencing increasing challenges in identifying, managing and responding to supply chain risks and vulnerabilities. Insolvency, international trade disruptions or other risks affecting critical suppliers can impact an asset's ability to continue operations efficiently. Further, complex supply chains can generate security risks such as entry points through compromised hardware products.

These consequences are considered in further detail in the following case studies from both Australian and international contexts.

Examples of disruptions to telecommunications assets – domestic and international

2022 Optus data breach	Cyber Risk
Situation: In September, 2022, Optus suffered a cyber-attack which led to the theft of customer data. The breach occurred due to an unsecured application interface that allowed other devices and systems to access it.[2] The stolen customer data contained personal information data such as addresses, Medicare information, passport information and driver licences.	
Outcome: The incident impacted approximately 10 million current and former Optus customers to varying degrees, with some having to replace several identification documents following the breach. In November 2022, Optus announced it had made a provision for exceptional expenses of $140 million for action to prevent harm to customers.[3] A class action seeking damages for impacted customers was launched in 2023 with over 100,000 participants, claiming that Optus breached consumer and telecommunications law and failed its duty of care to protect its customers' information. The class action may cause additional direct impacts to Optus.[4]	
Identified Gap: The impact of the Optus data breach on its customers highlighted a greater need for adequate risk management processes and stronger systems to improve the resilience of networks to data breaches and improve the reliability of networks.	

2022 Cyber-attack on Satellite Network in Ukraine[5]	Cyber Risk
Situation: On February 24, 2022, a cyber-attack disrupted broadband satellite internet access throughout Ukraine. This attack disabled modems that communicate with ViaSat Inc's KA-SAT, a critical Ukrainian satellite network, which supplies internet access to tens of thousands of people in Ukraine and Europe. The attack was deliberately designed to disrupt Ukrainian command and control services. The remote malware deployed in the system created impacts throughout Europe, by remotely erasing software on modems and routers making them non-operational.	

[2] Optus data breach, Queensland Government, 2022, qld.gov.au/community/cyber-security
[3] Optus Half Year results, Optus, 2022, optus.gov.au/content-documents
[4] Slater and Gordon commences class action against Optus over data breach, Slater and Gordon media release, 2023, slatergordon.com.au/media
[5] Case Study: Viasat Attack, cyberconflicts, 2022, cyberconflicts.cyberpeaceinstitute.org

Outcome: The attack impacted telecommunications systems, threatened government and military objects, and impacted civilian objects both in Ukraine and beyond when they experienced a loss of internet access and disruptions to energy systems. While most network users were back online after several days, some users reported that their internet access was unavailable for more than two weeks.[6]

Critical infrastructure throughout Europe was impacted, including a German energy company who lost remote monitoring access to over 5,800 wind turbines. In France, nearly 9,000 subscribers of a satellite internet service provider experienced outages. An additional 13,000 subscribers of other satellite internet service providers across Hungary, Greece, Italy, and Poland were affected.

Identified Gap: This case study demonstrates the need for regulation to consider all hazards, including from malicious actors that could disrupt a network. Telecommunications assets should be required to anticipate and respond to disruption by malicious actors, including undertaking risk management activities which may prevent or mitigate flow on impacts.

2019-2020 Bushfires Impact on Major Australian Telecommunication Networks	**Natural Hazard**

Situation: In 2019–20, unprecedented fires swept across Australia's south-east coast. The fires impacted many communities and critical services, including telecommunications. These disruptions created significant challenges for individuals and communities seeking emergency assistance and access to Government-issued emergency alerts, as well as general welfare communications.[7]

Outcome: The magnitude of the fires saw significant damage to physical telecommunications assets. It was reported that 1,390 facilities were impacted, with the average outage lasting 3.5 days.[8] Prolonged power outages created major disruption, including for those seeking to aid recovery. Loss of network coverage meant that people were unable to receive emergency messages about the location of fires. This affected people's ability to make decisions about preparing their properties, whether to evacuate, and where to evacuate to. Emergency services had reduced communications and had to rely on radiocommunications in many instances.[9]

Identified Gap: Consistent regulatory standards across all critical infrastructure assets may mitigate the impact of mass outages, including through enhancing knowledge and understanding of the incident response mechanisms available where a risk to a telecommunications asset is realised.

[6] KA-SAT Network cyber attack overview, 2022, news.viasat.com

[7] Final-Report-of-the-NSW-Bushfire-Inquiry.pdf, NSW Government, nsw.gov.au

[8] Impacts of the 2019-20 bushfires on the telecommunications network, ACMA, 2020, acma.gov.au; Final-Report-of-the-NSW-Bushfire-Inquiry, NSW Government, nsw.gov.au

[9] Impacts of the 2019-20 bushfires on the telecommunications network, ACMA, 2020, acma.gov.au; Final-Report-of-the-NSW-Bushfire-Inquiry, NSW Government, nsw.gov.au

2022 Outage of Critical Japanese Mobile Carrier	Supply Chain Risk
Situation: On July 2, 2022, KDDI Corp, Japan's second-largest mobile carrier, experienced a network disruption. The disruption lasted for more than 60 hours and impacted more than 40 million mobile customers' (including 260,000 corporate users) ability to make phone calls and access internet services.[10]	
Outcome: Investigations found the disruption occurred as a result of a malfunction in equipment used for voice call services. Beyond the direct impacts felt by KDDI Corp's customer base, the outage created significant flow on impacts to other essential services. This included, for example, disruption to weather service providers reliant on KDDI's network, temporary cessation of postage services and parcel deliveries, inability to access ATMs and use network-connected vehicles.[11] Payment systems were also affected by the outage.[12]	
Identified Gap: This case study highlights the importance of regulatory frameworks which enhance industry-wide resilience through consistent risk management activities. Where reliance on a single provider can be reduced, and adequate risk management mechanisms are in place, the impacts of disruptions can be mitigated.	

Outline of four key hazard domains

Hazard Domain	Identified Risk	Hypothetical Example
Physical & Natural	Increased occurrence of extreme weather events and natural disasters including heatwaves, bushfires and floods means that telecommunications assets are exposed to natural hazard risks. These risks have the potential to damage both physical infrastructure and remote systems.	Floods can cause significant disruptions to telecommunications assets including, reduced ability to deliver and support critical services following disaster events until connectivity is restored.
Supply chain	Disruptions to telecommunications assets' supply chains can affect Australia's social and economic stability, defence, and national security, as well as the reliability and security of other critical infrastructure assets. This risk is magnified where organisations are primarily reliant on supplies that are sourced internationally.	A telecommunications provider may be reliant on a sole or limited number of third-party suppliers for critical hardware components used in the operations of its assets. Where this major supplier faces disruptions, the quality, security, and ability to provide telecommunication services may be compromised. This may lead to widespread service disruptions for many customers if the supplier's component was unable to be delivered or malfunctions (and no alternative is available).

[10] KDDI aims to restore service, Reuters, 2022, reuters.com/business/media
[11] Telecom network outages, the ESG risks of a connected world, 2022, Sustainalytics, Sustainalytics.com.esg-research
[12] KDDI aims to restore service, Reuters, 2022, reuters.com/business/media

Hazard Domain	Identified Risk	Hypothetical Example
Personnel	Personnel with advanced knowledge, access to systems, data or premises may pose insider threat risks including espionage, infrastructure sabotage and misuse of sensitive data.	An employee may access sensitive information or compromise network availability. This could result in theft or exposure of sensitive information. The telecommunications provider may face consequences such as service disruptions, data breaches, reputational damage and legal liability.
Cyber	Telecommunication assets are vulnerable to thousands of attempted cyber-attacks every day. Due to constant improvements in infiltration capabilities, it has become easier to carry out destructive cyber-attacks.	A telecommunications provider faces a cyber-attack by a group of malicious actors who aim to disrupt communication networks and steal sensitive data. The attack exploits vulnerabilities within the company's software, network and employee devices to gain unauthorised access to company data.

Existing legislation related to Telecommunications assets and entities of the Australian Telecommunications Sector

	Overview of Regulation	Identified Gaps
Security of Critical Infrastructure Act 2018	The SOCI Act manages national security risks in Australia's critical infrastructure assets. The SOCI Act applies to eleven sectors including communications, data storage and processing and energy. The SOCI Act establishes: • the requirement to adopt and maintain a written risk management program; • reporting requirements in the event of cyber incidents which impact on the availability, integrity, reliability, and confidentiality of the asset to the Australian Cyber Security Centre; • obligations to provide operational and ownership information to the Register of Critical Infrastructure Assets; • last resort government assistance measures for incident response. • measures to protect sensitive information about critical assets; • enhanced Cyber Security Obligations' applied to 'Systems of National Significance' (SoNS).	Critical telecommunications assets are not currently subject to obligations under the SOCI Act, except any enhanced cyber security obligations that are applied to declared SoNS. Where they are not SoNS, critical telecommunications assets are currently only subject to the obligation to notify data storage providers if they store or process business critical data.

	Overview of Regulation	Identified Gaps
Telecommunications Act 1997	The *Telecommunications Act 1997* (Tel Act) establishes a regulatory framework for carriers and carriage service providers. Carriage services are defined as services for carrying communications by means of guided and/or unguided electromagnetic energy. The Act imposes obligations for: • protecting the privacy of communications; • preventing telecommunications networks to be used to commit offences; and • facilitating the use of carriage services for defence purposes or the management of natural disasters. Additionally, Part 14 sections 313(1A), 314A & 314B, and sections s315A, 315B and 315C require telecommunication providers to do their best to protect the security of their networks and facilities, including to stop their use in criminal acts. Under Part 14, the ACMA can investigate and take enforcement action if providers fail to comply with obligations and improperly use information and documents that come into their possession in the course of their business which relate to the contents of a communication: • that has been or is being carried; • was supplied by the carriage service; or • details a person's personal affairs. Sections 313(1A), 314A and 314B, and section 315A under the Tel Act will be integrated into the SOCI Act through these reforms.	The Tel Act imposes a diverse range of responsibilities on carriers and carriage service providers, particularly in relation to privacy and in states of emergency. However, the Act does not include any specific requirement to develop and implement risk management programs. While interim reporting obligations have been switched on under Tel Act, there are generally no reporting obligations on captured entities. The Act instead mandates that providers submit information to the Register of Critical Assets or comply with Mandatory Cyber Incident reporting.

Overview of Regulation		Identified Gaps
Privacy Act 1988	The *Privacy Act 1988* (Privacy Act) dictates how personal information in the federal public sector and in the private sector can be collected, used, stored, and disclosed.	The Privacy Act is the primary lever for the protection of personal information, given its unique ability to regulate the large-scale collection and distribution of data. While it provides avenues for individuals to complain about alleged interferences with their privacy by service providers, it does not impose positive obligations on telecommunications providers to create and implement risk management protocols.
Radiocommunications Act 1992	The *Radiocommunications Act 1992* regulates the planning, allocation, and use of radiocommunications. The Act provides for: • radio frequency planning; • licencing and registration of radiocommunications; • re-allocation of parts of the spectrum; and • general regulatory requirements extending to equipment rules, interference with radiocommunications and dispute management.	Complaints can be made to the Australian Communications and Media Authority (ACMA) where there is an interference or risk of interference or disruption to radiocommunications. While ACMA has a range of powers to respond to risks, there is no requirement to create a risk management program or reporting requirement. Similarly, licence holders have a compliance reporting obligation to the ACCC, but this does not extend to risk management protocols.
Telecommunications (Interception and Access) Act 1979	The *Telecommunications (Interception and Access) Act 1979* (TIA Act) makes it an offence to intercept or access private telecommunications without the knowledge of those involved in that communication, except for law enforcement or national security purposes.	While the TIA Act does impose risk minimisation duties on the Director-General of Security in relation to the issuance of foreign communications warrants, as well as on ACMA in granting exemptions for trial services, there is no specific requirement for risk management protocols for telecommunications sector disruptions.
Foreign Acquisitions and Takeovers Act 1975	The *Foreign Acquisitions and Takeovers Act 1975* mandates that foreign individuals must obtain approval to operate or own telecommunications services in Australia.	The Act provides last resort powers to deal with foreign investment-borne national security risks and to penalise officers where there were high risks of contravention of the Act. However, the FATA is not designed to directly consider the risk management activities of Australia's critical infrastructure and cannot address the identified gaps.

Existing standards, guidelines, and regulators for Australia's telecommunications sector

Organisation	Standards & guidelines
Department of Infrastructure, Transport, Regional Development, Communication and the Arts	Telecommunications (Carrier Licence Conditions – Security Information) Declaration 2022 Telecommunications (Carriage Service Provider – Security Information) Determination 2022
The Communications Access Co-ordinator (within the Attorney-General's Department, under TIA Act)	Interception capability plan to be lodged annually by 1 July

Jurisdiction	Regulators
Commonwealth	Department of Home Affairs Department of Infrastructure, Transport, Regional Development, Communication and the Arts Australian Communications and Media Authority (ACMA) Australian Competition and Consumer Commission (ACCC) Telecommunications Industry Ombudsman Australian Information Commissioner Attorney-General's Department Communications Alliance

Costing process completed by responsible entities for critical telecommunications assets

Industry participants were consulted on the proposed regulatory changes and rules from Q1 2024. Feedback from the initial consultation was incorporated into this Supplementary Analysis.

To assess the potential cost implications of the proposed regulatory changes, an additional consultation period was held between 15 December 2024 and 14 February 2025. This consultation period sought submissions from Industry participants on the cost impacts of the proposed regulatory changes. This additional consultation resulted in limited engagement and no submissions on the estimated cost impact. Noting the nil response, the Department has adopted a qualitative analysis of the potential impacts to industry and the broader economy of the proposed regulatory option.

This qualitative assessment will draw on the previous analysis from the 2022 Regulatory Impact Assessment (RIS) of the then proposed regulatory changes to the SOCI Act. It is estimated that the cost to implement the regulatory changes for critical telecommunications assets would not be more than, and is likely to be less than, that of the regulatory changes for other critical infrastructure assets (and which were examined in the 2022 SOCI RIS).

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 cost of regulation will be borne by responsible entities for critical telecommunications assets who meet the threshold in the Rules. The direct costs of regulation have been assessed against the cost impact rating scale in the table below. For each element of the proposed regulatory change, an assessment of the scale of cost impact to industry has been made.

Community organisations and individuals will not be directly affected but there will likely be indirect costs passed onto consumers. Without quantification of the direct cost impact, an assessment of the indirect impact is difficult. For the purposes of this Supplementary Analysis, consideration of the indirect impact has been limited to commentary on the economic analysis undertaken for the other critical infrastructure asset classes examined in the 2022 SOCI RIS.

Cost impact rating scale

Cost Impact Rating	Description
Low	The required uplift or change to an entity's processes, capability, governance and systems is minor. The requirements of SOCI are being substantively met by current activities and consequently, the marginal cost of implementing and maintaining compliance with the SOCI obligations is Low.
Moderate	The required uplift or change to an entity's processes, capability, governance and systems is significant in some but not all areas of the business. The requirements of SOCI are being partially met by current activities and consequently, the marginal cost of implementing and maintaining compliance with the SOCI obligations is Moderate.
High	The required uplift or change to an entity's processes, capability, governance and systems is significant in most areas of the business. The requirements of SOCI are not being met by current activities and consequently, the marginal cost of implementing and maintaining compliance with the SOCI obligations is High.

Assessment of cost impact to critical infrastructure assets

Proposed changes	Cost Impact Rating	Rationale
Introduce an all hazards critical infrastructure risk management program	Moderate	The introduction of the critical infrastructure risk management program would require industry to uplift current practices to ensure compliance with the SOCI Act. Existing telecommunications security requirements already require risk mitigation, particularly against sabotage and espionage and cyber security. The CIRMP is an all-hazards obligation, so some uplift is still required. It is therefore assessed that this broader obligation would have a moderate impact to industry.

Proposed changes	Cost Impact Rating	Rationale
Addition of new reporting requirements to ensure compliance with the amended regulations.	Low	This change would require industry participants to produce a board or equivalent attested report annually on their written CIRMP. Noting the frequency of this and that most (or all) affected entities will already have significant risk management activities in place, this change has been assessed as having a low impact.

Based on the above assessment, it is estimated that the cost to implement the regulatory changes for critical telecommunications assets would not be more than, and is likely to be less than, that of the regulatory changes implemented for other critical infrastructure assets (and which were examined in the 2022 SOCI RIS). Given the existing regulatory framework established by the Tel Act, owners of critical telecommunications assets are already subject to security obligations involving risk management and reporting requirements. While the SOCI Act integrates and uplifts these obligations to an all-hazards framework, it is assessed that the cost impact will be lower than for other classes of critical infrastructure asset because the processes, capabilities, governance and systems required to comply with the new obligations will only require uplift rather than establishment. For most entities this will result in a lower cost impact relative to the estimated costs presented in the 2022 SOCI RIS.

In this context, a summary of the cost impact data collected during the 2021-22 consultation period[13] is provided below.

Regulatory cost per entity from 2021-22 consultation period (indexed to December 2024)

Critical infrastructure asset	Costs ($ million)	
	Average one-off cost per entity (submissions)	Average annual ongoing cost per entity (submissions)
Critical electricity assets	9.3	4.4
Critical gas assets	12.1	2.4
Critical water assets	16.5	7.0
Critical data processing or storage assets	2.0	2.2
Critical broadcasting and domain name system assets	0.8	0.6
Critical financial market infrastructure assets (payment systems)	0.1	1.6
Critical liquid fuels assets	10.2	3.0
Critical hospitals	14.9	11.6
Critical energy market operator assets	25.4	7.7

[13] Information about the methodology for calculating the costs from 2021-22 consultation period can be found in the 2022 RIS here.

Critical freight infrastructure *and* critical freight services assets	4.5	2.6
Critical food and grocery assets	3.6	2.0
Total average cost per entity	**9.0**	**4.1**

Benefits of option 2

Reliable and continuous access to telecommunications assets is critical for Australia's prosperity. The critical infrastructure risk management program framework will uplift baseline security across all captured critical telecommunications assets to ensure more resilience to hazards. Its primary benefit is that compliance with the risk management program reduces the frequency and intensity of incidents, which has cascading whole of economy benefits by minimising supply disruptions and economic shocks.

Economic impacts of disruptions to telecommunications assets

Disruptions to critical telecommunication assets can have profound effects, both directly on customers and as other critical infrastructure assets are unable to use telecommunications networks to perform essential services. These events generate costly immediate and longer-term impacts on the Australian economy. Further, telecommunications assets hold significant quantities of data including highly sensitive data about all Australians and entities. As such, telecommunications assets may be more frequently exposed to risks involving attempted espionage and sabotage than other critical infrastructure assets.

A significant incident affecting a critical telecommunications asset may cause:

- disruptions to economic activity, with immediate impacts on other critical infrastructure or government services (e.g. financial intermediaries, health, and transport services);
- self-perpetuating economic shocks through the supply chain if redundancies are unavailable or inadequate;
- compromises to sensitive data, including business critical data, which may generate further national security and privacy risks and severe opportunity costs as business efforts are redirected to consequence management; and
- impairments of the availability of networks causing wide-ranging communications difficulties for individuals, including but not limited to:
    - connecting with friends and family,
    - contacting health care and emergency services,
    - obtaining information or advice,
    - working from home, or
    - undertaking online educational courses.

Additionally, a disruption to telecommunications infrastructure can significantly affect the social well-being of Australia. The case studies above show that disruptions to telecommunications assets can have an amplified negative impact on communities during existing emergency situations such as floods and bushfires. Consequently, in addition to the costs to the economy of a disruption to telecommunication assets, there are the community costs of death, disease or, injury which are increased in consequence or likelihood because of an incident.

With Government and businesses increasingly storing and communicating large amounts of information on and across critical telecommunications assets, these assets have increasingly become a target for espionage, sabotage, and interference activity. In instances where this information is

unlawfully accessed, sensitive data, law enforcement operations, and the location of persons could be exposed.[14]

To support the assessment of the potential direct and indirect economic impacts of an incident to a critical telecommunications asset on the Australian economy, a series of case studies were included in this Supplementary Analysis. These case studies highlight that telecommunications 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 is clear from the case studies noted above that industrial and commercial sectors can be significantly impacted by telecommunication outages.

For the purposes of estimating the cost of a range of future avoided incidents in Australia, an incident impacting a 'Major Telecommunications Carrier' was used. Given the magnitude of damages, this incident is considered a moderate risk scenario. The use of an incident modelled on an actual event to define a baseline risk point of comparison is important because it ensures the benefits analysis is grounded in reality.

Based on this, a framework for considering the potential impacts of Australian telecommunication asset outages following failure of critical infrastructure is provided in the table below.

	Severe scenario	Moderate scenario	Low scenario
Intensity of event	200% of moderate scenario	Incident impacting Major Telecommunications Carrier	50% of moderate scenario

As noted above, the economic impact of an incident will vary due to a range of factors including the location and type of incident, as well as its timing and duration. 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. Due to this, this analysis may not incorporate all direct costs incurred by all future incidents.

	Scenario 1 (Severe) $ million	Scenario 2 (Moderate) $ million	Scenario 3 (Low) $ million
Total direct cost to the economy of the incident	$280	$140	$70
Total in-direct costs to the economy of the incident	50-75% of the direct cost.		

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.).It is estimated that there would be additional indirect costs of an incident due to both the upstream and downstream of the supply chain impacts. Based on the economic modelling undertaken for other classes of critical infrastructure assets in the 2022 RIS, the additional indirect costs could range from 50-75% of the total direct costs of an incident.

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

[14] ParlInfo - Telecommunications and Other Legislation Amendment Bill 2017 (aph.gov.au)

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, the frequency and severity of all hazard risks for telecommunication assets are growing. While some events of the magnitude described in this Supplementary Analysis 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 cost for critical telecommunications assets is likely to be less than for the other classes of critical infrastructure asset examined in the 2022 SOCI RIS because the Tel Act already requires some of the processes, capabilities, governance and systems which will be required by rules and obligations established by the SOCI Act. This, together with the increasing frequency of incidents, 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 telecommunication assets; and
- ensuring that adoption of the risk management program framework for telecommunication assets is reasonable and proportionate to the purpose of the program;

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