INDEPENDENT REVIEW OF THE SECURITY OF CRITICAL INFRASTRUCTURE ACT 2018

DR JILL SLAY AM

I acknowledge the Traditional Custodians throughout Australia and their continuing connection to land, sea and community. I acknowledge the Kaurna peoples, the Traditional Custodians of the land on which this report was prepared, and I pay my respects to their Elders, past, present and emerging.

2 February 2026

The Hon Tony Burke MP
Minister for Home Affairs, Minister for the Arts, Minister for Cyber Security,
Minister for Immigration and Citizenship and Leader of the House
House of Representatives
Parliament House
Canberra ACT 2600

Dear Minister,

Further to my appointment as Independent Reviewer, I am pleased to present the report of my review of the *Security of Critical Infrastructure Act 2018*.

Thank you for the opportunity to conduct this review.

Yours sincerely,

Dr Jill Slay AM

TABLE OF CONTENTS

Contents

EXECUTIVE SUMMARY

INDEPENDENT REVIEW OF THE SECURITY OF CRITICAL INFRASTRUCTURE ACT 2018

This independent review, conducted by Dr. Jill Slay between November 2025 and January 2026, assessed whether Australia's *Security of Critical Infrastructure Act 2018* (SOCI Act) is achieving its intended objectives, functioning as intended, and is not producing unintended consequences. The review examined the SOCI Act's operation through comprehensive stakeholder engagement including 50 written public submissions, surveys from 89 respondents, interactive roundtables with over 600 participants, federal government department submissions, and international legislative comparisons.

KEY FINDING: MAJOR LEGISLATIVE CHANGE REQUIRED

The overarching conclusion is that the SOCI Act requires major legislative change to remove complexity and confusion while becoming more agile and responsive.

STRENGTHS ACKNOWLEDGED

Stakeholders consistently acknowledged that the SOCI Act has:

- increased executive and board-level awareness of infrastructure vulnerabilities
- established baseline governance frameworks and accountability structures
- improved asset visibility and incident reporting mechanisms
- created a common language for discussing critical infrastructure risks across sectors.

Australia and Singapore maintain the most mature critical infrastructure frameworks globally, both operational since 2018 with established compliance cycles and active enforcement.

CRITICAL IMPLEMENTATION CHALLENGES

Stakeholder feedback revealed a need for clarity in the SOCI Act, for the removal of regulatory duplication and visible enforcement action and clearer accountability mechanisms.

EMERGING THREAT GAPS

The majority of respondents believe the SOCI Act is not equipped to handle emerging threats:

- Artificial Intelligence (AI) and quantum risks (such as AI-enabled attacks, offshore AI dependencies, data poisoning, quantum cryptography vulnerabilities) are not explicitly addressed
- physical threat vectors including unauthorised drones and space-based service dependencies introduce unaddressed vulnerabilities
- cyber-heavy focus neglects physical security, personnel security, and all-hazards supply chain resilience.

The SOCI Act is perceived as too reactive and too slow compared to evolving risks, despite multiple previous modifications.

INTERNATIONAL COMPARISON INSIGHTS

The literature review highlighted the United Kingdom's (UK's) holistic approach, which explicitly recognises social cohesion as equally critical to national security as physical infrastructure itself. Social cohesion is identified as a 'centre of gravity' that, if disrupted, significantly weakens national resilience. Australia could consider adopting similar perspectives to strengthen public understanding and support for critical infrastructure protection.

PROPOSED GOVERNMENT AMENDMENTS

The Department of Home Affairs (the Department) released proposed amendments to the Critical Infrastructure Risk Management Program (CIRMP) Rules during the review period. These amendments represent a positive evolution from principles-based risk awareness toward demonstrable, intelligence-informed risk treatment. Key enhancements include mandatory uplift to Maturity Level 2, supply-chain vulnerability mapping, personnel security plans with mandatory AusCheck background checking, specified risk advice requirements, and explicit Foreign Ownership, Control or Influence (FOCI) risk management.

KEY AREAS OF STAKEHOLDER CONSENSUS

Key areas of consensus include:

- expanding SOCI Act scope to include AI services, content delivery networks, hyperscale cloud providers, drones, and space assets
- harmonising frameworks by aligning the SOCI Act with Australian Prudential Regulation Authority (APRA), Australian Securities and Investments Commission (ASIC), International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Cross-industry Prudential Standard 234 (Information Security) (CPS234), Protective Security Policy Framework (PSPF), and state regimes
- adopting a 'report once' model for incident reporting
- improving guidance through prescriptive, practical materials with worked examples, CIRMP templates, and plain-language guides (similar to ASIC regulatory guides)
- strengthening assurance by shifting from procedural audits to effectiveness-based reviews, with maturity-based tiering that rewards strong security posture
- enhancing capability through investment in protective security education, workforce training, and structured cross-sector threat intelligence sharing
- mandating bidirectional information exchange between government and operators (similar to the United States' (US) Cybersecurity and Infrastructure Security Agency (CISA) (CISA 2015).

KEY AREAS OF GOVERNMENT STAKEHOLDER DISCUSSION

Key areas of discussion included a range of topics:

- **All sectors**: Issues relating to foreign ownership were raised by many stakeholders, with some identifying potential national security risks as a result. Other stakeholders acknowledged that whilst foreign owned entities may present a risk, foreign ownership is not the only vector available to exert foreign influence, with many vectors falling outside direct SOCI Act regulation. Risks associated with FOCI are present across critical infrastructure, commonly in areas such as supply chain, where there is no appropriate domestic alternative. The SOCI Act should be designed to deal with the wide variety of FOCI risks, noting the risk of foreign ownership is predominantly managed through the *Foreign Acquisitions and Takeovers Act 1975*. It should be noted that SOCI-Act regulated entities have a wide range of organisational structures, including large multinationals, foreign owned investments, state owned enterprises, large domestic organisations and small and medium businesses. As a result, many of them are subject to multiple legislative requirements, which must be met prior to operating in the Australian market. Some stakeholder feedback focused on the perception that investment into the Australian market was challenging, given the potentially multiple layers of regulation to move through, with some stakeholders perceiving that there were unequal obligations which prevented their further investment. It appears some of this relates to the perceived lack of compliance action, with entities concerned that whilst they were complying (at a cost to their business) their

competitors were not. Per my recommendations, consideration should be given to reducing legislative duplication where possible and increasing compliance action when appropriate.

- **Energy sector**: another major issue that requires thought is that of the Electricity sector during a time of transition to renewables. The SOCI Act applies to generators larger than 30 Megawatts (MW). Thus, it is necessary to amend the SOCI Act to place cyber obligations (e.g. Australian Energy Sector Cyber Security Framework (AESCSF) as developed by the electricity industry) directly on inverter Original Equipment Manufacturers (OEMs). Alternatively, it might be necessary to require transmission networks or generators to report whether and how they pass obligations through the supply chain to OEMs and others. Aggregators and Virtual Power Plant (VPP) operators are also major attack surfaces and have no obligations under the SOCI Act, even if aggregated generation exceeds 30 MW.

- **Compliance challenges**: there is tension between a 'helping hand' approach versus stricter enforcement given the severity of national security threats.

- **Sector and asset class definitions**: other issues have arisen in debate with Trusted Information Sharing Network (TISN) groups and individual federal government departments over the breadth of critical infrastructure sectors and asset classes, and the need to enhance and expand both the sectors and asset classes where definitions do not match current context and/or practice. Examples of this include the Higher Education and Research sector and the response of some universities who have concluded that none of their research involves critical infrastructure. This issue is very worrying since universities face foreign interference risks, particularly around research security and the large number of international Science, Technology, Engineering and Maths (STEM) students. University foreign interference guidelines are now considered static and inconsistently applied and are problematic since they are voluntary rather than mandated. It might be necessary to consider a new definition of Higher Education and Research to encompass all forms of Higher Educational research and institutions such as Commonwealth Scientific and Industrial Research Organisation (CSIRO), National Health and Medical Research Council (NHMRC) and other medical research, co-operative research centres and projects and Defence funded research carried out in universities.

- **Newer sectors**: some critical infrastructure sectors and their asset classes are new or not 'switched on' and so it may be necessary to give deeper thought to, for example, how to redefine Healthcare and Medical as a sector and consider which assets are critical; this might be deeply connected to the medical supply chain and need cross-sector input. Other issues arise with the use of internationally based satellite services across regional and remote Australia. Many critical infrastructure sectors in regional and remote areas rely on such services which are not covered by the SOCI Act.

- **Self-attestation**: self-attestation by company boards on their risk management programs remains common. Concern was expressed that the approach has not evolved significantly since 2005, with cyber reporting still largely voluntary and ad hoc. There was some acceptance of introducing an appropriately qualified expert into the process to provide external assurance, such as an individual with a chartered cyber engineering qualification or a Certified Professional (CP) Cyber or an individual at operator level with suitable SOCI Act training at Certificate Level III or equivalent.

CRITICAL CULTURAL OBSERVATION

A notable finding was that most respondents deeply immersed in SOCI Act compliance lack emotional connection to defending and protecting Australia and its citizens. Exceptions came primarily from those with Defence and intelligence backgrounds. This disconnect between compliance obligation and national security purpose warrants departmental examination of the relationship between the protection of critical infrastructure and the role critical infrastructure plays in a cohesive society.

The SOCI Act has successfully established Australia as a global leader in critical infrastructure security governance. However, its current complexity, regulatory overlap, weak enforcement posture, and gaps in addressing emerging threats necessitate comprehensive legislative restructure rather than further incremental amendment. The SOCI Act must transition from compliance-driven to outcome-driven, with genuine security uplift as the goal. This review recommends accepting the proposed CIRMP amendments while pursuing broader legislative simplification to create permanent, agile, and responsive critical infrastructure protection suited to Australia's unique geopolitical position and threat environment.

Independent review conducted by Dr. Jill Slay. Review Period: November 2025 – January 2026.

SUMMARY OF RECOMMENDATIONS

RECOMMENDATION 1: Remove all possible Commonwealth regulatory duplication from the SOCI Act to produce harmonisation and reduce administrative burden.

RECOMMENDATION 2: Move from a 'light touch' compliance approach with a focus on administration and documentation to that of a penalty-based risk management process with the real enforcement of penalties**.**

RECOMMENDATION 3: Develop ASIC-style regulatory guides with worked examples, templates, and plain-language materials. Examine international approaches to industry peer committees and guides to support all regulated entities.

RECOMMENDATION 4: Home Affairs to work with the TISN community, Australian Signals Directorate (ASD), the Australian Security Intelligence Organisation (ASIO), the National Cyber-Security Co-ordinator, the Department of Industry, Science and Resources (DISR), particularly the Space Agency, and the Department of Foreign Affairs and Trade (DFAT) Cyber Ambassador to respond to concerns on emerging technologies. Home Affairs to lead in examining the impact of AI, quantum, physical threat vectors and the role of Operational Technology (OT) Cybersecurity as they relate to the SOCI Act.

RECOMMENDATION 5: Enhance TISN capability through education and information sharing.

RECOMMENDATION 6: Accept the summary of amendments to the CIRMP rules while working toward simplification and rationalisation of the SOCI Act framework to develop a new simpler principles-based SOCI Act. This would have key obligations, offences and penalties, supported by rules to ensure flexibility and futureproofing, and underpinned by detailed thematic handbooks or rulebooks with the prescriptive detail on how to comply.

RECOMMENDATION 6(a): Issues to examine include:

Definitions: expand what counts as critical infrastructure (corporate groups, space assets, energy systems, healthcare/food supply). Consider whether new sectors or asset classes need to be added or modified.

Register: examine the need for better data quality and real-time sharing between agencies.

Information sharing mandate: require two-way threat information exchange between government and operators.

Risk management programs: allow faster security patches, extend background checks, add annual reviews and whistleblower protections.

Incident reporting: expand to cover all types of outages, include offshore operations.

TISN compliance: credit voluntary cooperation when enforcing penalties.

Systems of National Significance (SoNS): simplify declaration process, cover all hazards, allow temporary declarations of SoNS.

Ministerial Directions: give government earlier intervention powers for infrastructure risks.

Hosting certification: create a legal framework for protecting government data.

Assets under construction: protect infrastructure while it is being built.

High risk vendors: create power to ban dangerous technologies or suppliers.

Information sharing: clarify rules for sharing best practices without exposing sensitive information.

The SOCI Act and other federal legislation: the SOCI Act is effective and useful and should be enhanced and modified to include areas of national security which are currently dealt with by other legislation. The right tools should be used for national security legislation.

Energy sector: the SOCI Act was designed for traditional energy sources and may not adequately address the energy transition and emerging threats. Major concerns include supply chain risks, with key operational players not being captured by CIRMP requirements despite managing critical operations. Consider issues with generator limits, inverter OEMs and aggregators and VPP operators.

Education sector: consider a new definition of the Higher Education and Research sector to encompass all forms of Higher Education research and the institutions carrying out such research.

National security concerns: examine where, and why, there is limited authority to mandate actions which causes a reactive rather than proactive posture due to non-mandatory reporting, and inability to access critical information needed for threat response.

Self-attestation: consider self-attestation by company boards on their risk management programs which remains common. Consider introducing an appropriately qualified expert into the process to provide external assurance, such as an individual with a chartered cyber engineering qualification or a CP Cyber or an individual at operator level with a suitable SOCI Act training at Certificate Level III or equivalent.

CHAPTER ONE

CONTEXT OF THE SECURITY OF CRITICAL INFRASTRUCTURE ACT 2018

THE NATURE OF CRITICAL INFRASTRUCTURE AND ITS PROTECTION

Figure 1: Power outages and critical infrastructure

This chapter examines the nature of critical infrastructure and its protection.

Critical infrastructure refers to the physical and virtual systems and assets that are essential to a country's functioning, where their disruption would have severe consequences for national security, economic stability, public health, or safety.

Governments typically designate and protect critical infrastructure because attacks or failures, whether from natural disasters, cyber-attacks, terrorism, or technical breakdowns, could cause widespread harm. The specific sectors considered 'critical' can vary by country, but the concept is fundamentally about identifying what society absolutely needs to keep functioning.

In the context of this review, **supply chain** refers to the network of entities, processes, and resources used in the delivery of essential services or products to end users, clients or consumers. In Australia's regulatory context, supply chain security is crucial because any kind of disruption, referred to in the SOCI Act context as 'all-hazards', can compromise the delivery of essential services relied on by the country. Therefore, critical infrastructure operators must identify and manage all risks throughout their supply chains and not just develop expertise within the focus of their own sector.

Depending on context, the concept of supply chain includes:

- suppliers of necessary inputs to critical infrastructure operators such as raw materials, components, technology, and services
- transportation and logistics systems that enable the movement of these materials, components and items of technology which allow the provision of desired services
- storage and distribution facilities
- critical infrastructure operators themselves and
- other critical infrastructure sectors that rely on the primary operator such as energy for water treatment, or telecommunications for finance.

Table 1, below, shows interdependencies between each of Australia's 11 critical infrastructure sectors. While each of these sectors individually provides a service that needs to be maintained, this service could be disrupted by weather events, physical terrorism, cyber-attack or accidental damage.

These separate critical sectors then become a complex system because of their interdependencies and so, for example, hospitals need electricity, water treatment plants need communications networks, and financial systems need internet connectivity. These interdependencies mean that disruption to one sector can cascade into others and thus disrupt the complete Australian economy and its social cohesion.

Table 1: Dependencies between the critical infrastructure sectors in the SOCI Act

Sector	Primary dependencies	Secondary dependencies
Healthcare and Medical	Energy; Water/Sewerage; Communications; Transport; Data Processing	Banking/Finance; Higher Education; Food & Grocery; Defence; Space Technology
Water and Sewerage	Energy; Communications	Transport; Data Processing; Defence; Banking/Finance; Space Technology
Higher Education	Energy; Communications; Data Processing	Transport; Banking/Finance; Food & Grocery; Defence; Space Technology; Water/Sewerage
Food and Grocery	Transport; Communications; Energy	Banking/Finance; Data Processing; Water/Sewerage; Space Technology; Defence
Transport	Energy; Communications; Data Processing; Space Technology	Banking/Finance; Water/Sewerage; Defence; Food & Grocery
Banking and Finance	Communications; Energy; Data Processing	Transport; Space Technology; Defence; Water/Sewerage
Communications	Energy; Transport; Data Processing	Banking/Finance; Space Technology; Defence; Water/Sewerage
Space	Energy; Communications	Transport; Defence; Data Processing; Banking/Finance
Data Processing or Storage	Energy; Communications	Transport; Water/Sewerage; Banking/Finance; Defence; Space Technology
Energy	Transport; Communications; Data Processing	Banking/Finance; Defence; Water/Sewerage; Space Technology
Defence	Energy; Communications; Transport; Data Processing	Banking/Finance; Space Technology; Water/Sewerage; Food & Grocery; Higher Education

THE PURPOSE OF THE SOCI ACT

The SOCI Act is a national resilience governance framework rather than a cybersecurity law. Its fundamental purpose is to ensure that government has visibility on who owns and controls our critical infrastructure, assurance as to how risk to its functionality is being managed, and intervention options where the failure of infrastructure would have national and damaging consequences. The SOCI Act protects physical facilities, supply chains, information technologies and communication networks, as described above. If these were destroyed, degraded or rendered unavailable for extended periods, then Australia's social and economic wellbeing, national defence, or national security would be severely damaged. The SOCI Act operates on a functional basis: assets are regulated because of what they enable nationally, not because of the sectoral label of the organisation that operates them.

Since its commencement, the SOCI Act has undergone significant reform, including major amendments in 2021, 2022 and 2024, to respond to a rapidly changing threat landscape. These amendments expanded the SOCI Act's coverage to additional sectors, introduced obligations such as mandatory cyber incident security reporting, risk management programs, and enhanced cyber security requirements for systems of national significance. The cumulative effect of these successive reforms is a more robust but also more complex regulatory framework for industry and government to navigate.

Section 60A of the SOCI Act requires an independent review be conducted into the 'operation' of the SOCI Act and this report is that of the Independent Reviewer Dr Jill Slay.

KEY DEFINITIONS IN THE ACT

- **Critical infrastructure asset:** a single asset includes multiple parts functioning together as a system or network, including premises, computers, and data.
- **Responsible entity:** an entity that owns or is responsible for operating a critical infrastructure asset.
- **Direct interest holder:** an entity holding a legal or equitable interest in 10% or more of a critical infrastructure asset or having an interest that puts them in a position to influence or control that asset.
- **SoNS:** critical infrastructure assets deemed by the Minister of Home Affairs to require Enhanced Cyber Security Obligations (ECSO) due to their national importance.

SOCI AS A NATIONAL GOVERNANCE FRAMEWORK

From an operator perspective, the SOCI Act asks three fundamental questions:

- who is accountable for this asset?
- what are the material risks to national service delivery?
- can the operator manage a serious incident without government intervention?

The SOCI Act's obligations exist to provide credible answers to these questions.

MAIN OBLIGATIONS OF THE SOCI ACT

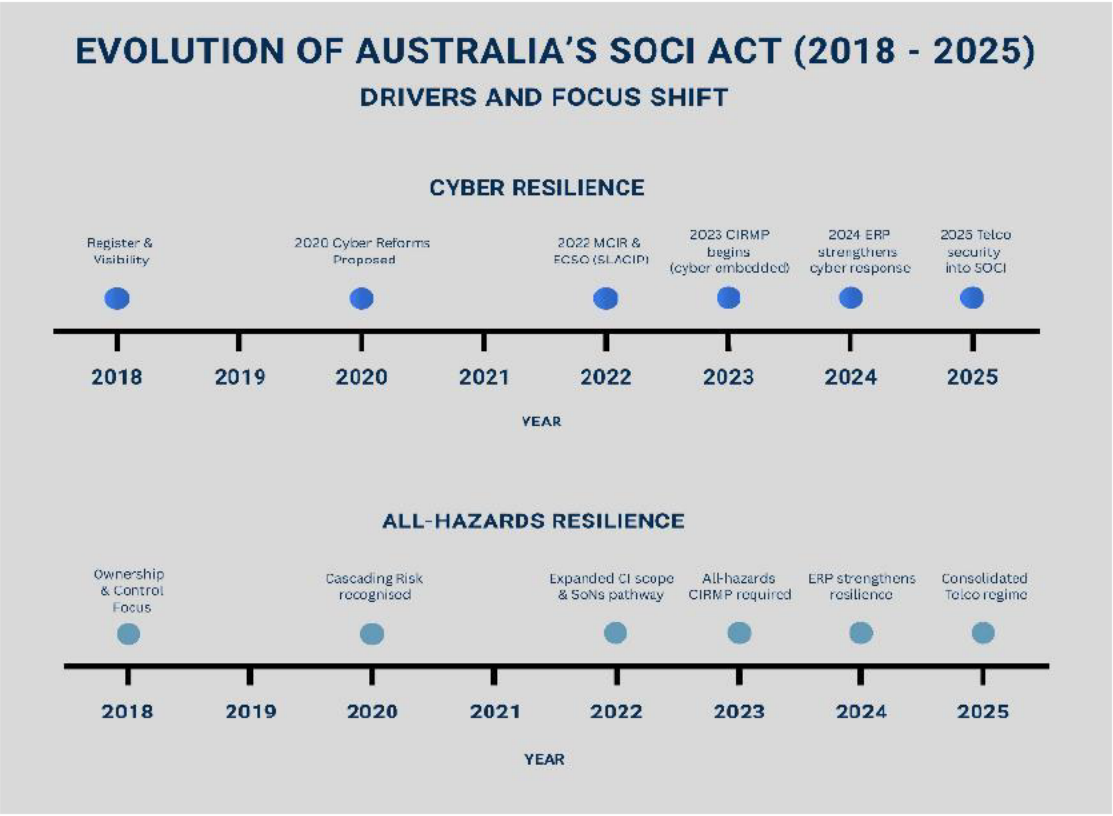
Table 2: Main obligations of the SOCI Act

Obligation	Detail
Register of Critical Infrastructure Assets (Part 2)	Responsible entities and direct interest holders must provide the Critical Infrastructure Security Centre (CISC) (within the Department) with operational, ownership, and interest and control information.
Mandatory Cyber Security Incident Reporting (Part 2B)	Responsible entities must report actual or imminent cyber security incidents to ASD: **Relevant impact:** Within 72 hours, they must provide a report on impacts on asset availability, integrity, reliability, or confidentiality of information. **Significant impact:** Within 12 hours they must provide a report on whether an incident materially disrupts provision or availability of essential goods or services.
Critical Infrastructure Risk Management Program (CIRMP) - Part 2A	Responsible entities in 13 designated asset classes must adopt, maintain and comply with a written CIRMP that takes an all-hazards approach across four key vectors: • physical security and natural hazards • personnel hazards • supply chain hazards • cyber security and information security hazards. **Key requirements:** The entity is obliged, among other things, to: • identify and mitigate material risks • comply with a designated or equivalent cybersecurity framework (including the AAESCSF) and meet specified maturity levels • provide annual reporting to regulators within 90 days after the financial year end. The CISC may direct a responsible entity to vary its CIRMP to address a serious deficiency posing material risk to national security, Defence, or social or economic stability.
Enhanced Cyber Security Obligations (ECSO) - for SoNS only	Assets designated as SoNS may face four additional obligations. Each obligation is separate and is individually applied to the asset. The ECSOs include: • developing cyber security incident response plans • undertaking cyber security exercises • undertaking vulnerability assessments • providing system information to ASD to develop a near real-time threat picture.

GOVERNMENT POWERS	
Information gathering and Direction Powers	The Australian government can request information from entities, and the Minister can issue directions to entities if there is risk of acts prejudicial to security. In cases of severe cyber threats, government can intervene to assist organisations or direct them to take specific actions, and in extreme cases, take control of certain aspects of the response.
Government Assistance Measures	The framework can be used in response to all types of incidents (not limited to cyber-related ones) reflecting the SOCI Act's all-hazards approach to risk.
Protected Information Provisions	It is an offence to disclose information about critical infrastructure assets unless the disclosure complies with the SOCI Act. Entities may now make a harms-based assessment to inform use and disclosure of information, and may make a record of, use or disclose protected information.

HISTORY OF DEVELOPMENT OF SOCI ACT

The SOCI Act (2018) began as an ownership-and-control visibility regime. From 2020 onward, escalating cyber threats and the recognition of interdependent, cascading failures drove reforms that added positive security obligations (incident reporting and risk management) and expanded the scope of critical infrastructure to include digital services. The 2024 Enhanced Response and Prevention (ERP) reforms further strengthened response and prevention mechanisms and, in 2025, telecommunications security was consolidated under the SOCI Act framework.



Taking a chronological overview of Australia's critical infrastructure security framework evolution, it has moved from basic visibility (knowing what exists) to proactive security requirements, and from managing risks to one of enhanced obligations for the most critical assets. Each phase built on the previous one rather than replacing it.

Figure 2: Evolution of Australia's SOCI Act (2018 – 2025)

OBLIGATION TIERS

Obligation tiers refer to the risk-based framework used in the SOCI Act and determine what security obligations apply to different critical infrastructure assets based on their importance and risk level.

- **Tier 1 (visibility)** functions as the foundation since one cannot protect what one does not know exists. This registration requirement creates a national inventory of critical assets and their interdependencies.
- **Tier 2 (proactive security)** adds two active obligations which are cyber incident reporting to ensure government awareness of threats to critical infrastructure in real-time, and the addressing of all-hazards (not just cyber), requiring systematic and ongoing risk management for specific asset classes.
- **Tier 3 (enhanced)** applies stricter controls to SoNS. These are the assets whose compromise would have catastrophic national consequences. ECSOs assist an entity to prevent, detect and respond to a cyber security incident.

Framework/standards alignment: The mapping to NIST, ISO 27001 and APRA CPS234 allows organisations to leverage existing control frameworks rather than building parallel compliance programs. This reduces duplication and helps demonstrate how existing security investments satisfy SOCI Act requirements. ERP measures and telecommunications consolidation in 2024 - 2025 illustrate more recent modification to the framework, particularly enhancing prevention and response capabilities.

KEY POINTS ABOUT ASSET CLASSES

Table 3: Key points about asset classes

Key concept	Description	Impact/implications
Not all obligations apply to all assets	The list of assets and sectors required to comply with each obligation may be different. Different asset classes have different obligations 'switched on'.	Organisations must understand which specific obligations apply to their particular asset class, not assume universal requirements.
Asset-specific definitions	Many asset classes have very specific criteria (revenue thresholds, passenger numbers, specific named facilities) that determine whether something qualifies as a critical infrastructure asset.	Qualification as critical infrastructure depends on meeting specific, measurable criteria unique to each sector.
Sector-specific responsible entities	The definition of 'responsible entity' can vary by sector and asset class.	Accountability and compliance obligations may rest with different parties depending on the sector.
Interconnected nature	Assets include multiple parts which function together as a system or network, including premises, computers, and data.	Critical infrastructure must be viewed holistically - protecting individual components without considering system-wide dependencies is insufficient.

Different obligations apply to different asset classes - not all obligations are ‘switched on’ for every asset class. Organisations must check which specific obligations apply to their asset class through the SOCI Act, associated Rules and CISC guidance materials. The complexity arises from the layered obligations, sector-specific requirements, and the interaction between registration, reporting, risk management, and enhanced security obligations for different types of assets. This is further explained in Appendix J.

CONCLUSION

The evolution of Australia's critical infrastructure security framework through the SOCI Act represents a fundamental shift in how the nation approaches resilience and national security. What began in 2018 as a relatively straightforward ownership-and-control visibility regime has matured into a comprehensive, risk-based, resilience governance framework that addresses the complex interdependencies and cascading vulnerabilities inherent in modern critical infrastructure systems.

The current framework embodies a sophisticated understanding of infrastructure resilience. It moves beyond traditional cybersecurity compliance to embrace an 'all-hazards' approach that acknowledges the full spectrum of threats from physical terrorism and extreme weather events to supply chain vulnerabilities, insider threats, and FOCI. The tiered obligation structure ensures that regulatory burden is proportionate to national risk, with basic visibility requirements for all designated assets, enhanced obligations for systems requiring active risk management, and the most stringent controls for SoNS.

The success of the SOCI Act framework thus ultimately depends on several key factors including regulatory coherence across government agencies, practical guidance to ensure that industry responses to identified risk are strategic rather than merely reactive and flexibility to accommodate rapid technological change and emerging threats without the constant need to amend the legislation in such an environment. As the threat environment continues to evolve, as infrastructure systems become more interconnected and complex, and as new sectors and technologies emerge as nationally significant, the framework will require continuous refinement.

CHAPTER TWO

INTERNATIONAL COMPARISONS ON CRITICAL INFRASTRUCTURE BREACHES AND LEGISLATIVE APPROACHES

CRITICAL INFRASTRUCTURE BREACHES

There is a large amount of academic, government and business literature focusing on critical infrastructure breaches internationally and, particularly, on aspects of the supply chain and operational technology (OT) systems that monitor and control physical devices, processes, and infrastructure in the real world. Some examples are referenced below to indicate trends, indicators of complexity and observed weaknesses.

There is a growing crisis in supply chain cyberattacks affecting UK, US and South-East Asian businesses, with 61% of UK industry experiencing such breaches in the past year. It is argued that modern organisations' reliance on interconnected systems and third-party providers creates multiple entry points for attackers, who increasingly target smaller suppliers as the easiest route into well-defended enterprises. Notable examples include attacks on major retailers like Marks & Spencer, Co-op, and Harrods, as well as Jaguar Land Rover's production halt due to a cyber breach. A recent TechRadar (2025) article highlights a dangerous disconnect between organisational confidence and actual preparedness, recommending three key steps: embedding holistic security in partnership agreements, implementing continuous people vetting, business and security audits, and strengthening internal cyber defences.

Dr. David Mussington (previously of the US CISA) provided an analysis of the Earth Ammit threat actor (attributed to China) and examines two linked campaigns, VENOM and TIDRONE, that demonstrate sophisticated supply chain compromise targeting Taiwan and South Korea's drone, satellite, and defence manufacturing sectors. The threat actor compromised upstream software and enterprise resource planning providers to inject malicious updates into downstream environments, particularly targeting military organisations, satellite/drone manufacturers, and defence-adjacent payment platforms. From a critical infrastructure perspective, the campaigns reveal how ‘enterprise Information Technology (IT)’ systems now constitute strategic battlespace for Low Earth Orbit (LEO) resilience and intelligence, surveillance, and reconnaissance (ISR) continuity. The analysis emphasises that compromised enterprise resource planning systems could enable adversaries to alter firmware, exfiltrate operational data (maintenance schedules, deployment plans, asset locations), and map dependencies between ground segments and LEO constellations. This pre-positioned access could degrade ISR and drone capabilities during crises, particularly in Indo-Pacific conflicts. Mussington argues that LEO security must extend beyond satellites to include business systems managing constellations, and recommends treating key vendors as critical infrastructure, demanding software bills of materials, implementing zero trust architecture, and conducting tabletop exercises based on supply chain compromise scenarios.

The 2025 SANS (a large US and international SysAdmin, Audit, Network, and Security cybersecurity training provider) survey of 330 Industrial Control System (ICS) /OT security professionals reveals that 22% of organisations experienced cybersecurity incidents in the past year, with 50% originating from unauthorised external access and 40% causing operational disruption. Key findings indicate that only 14% of organisations feel fully prepared for emerging threats, only 13% have implemented advanced remote access controls, and coverage gaps exist across the Purdue Model (model used to secure cyber-physical aspects of OT security) with minimal visibility at lower operational levels. The survey shows that regulation drives security maturity and regulated sites experienced 50% fewer financial losses and safety impacts despite similar incident rates. Organisations are prioritising investments in asset visibility (54%), threat detection (43%), and secure remote access (40%) for 2026-2027, with both regulatory requirements and evolving threats serving as primary drivers.

The World Economic Forum Global Cyber Security Outlook of 2025 indicated supply chain vulnerabilities are a primary concern looking forward to 2026:

- **54% of large organisations** identify supply chain challenges as the greatest barrier to achieving cyber resilience
- supply chain complexity has emerged as the **top cybersecurity risk from an ecosystem perspective**

- key concerns include **software vulnerabilities** introduced by third parties and cyber-attack propagation throughout ecosystems.

The report identifies several high-risk critical infrastructure sectors facing unprecedented threats including:

1. **water facilities**: cyber-attacks pose significant risks to public safety. The October 2024 attack on the largest US water utility highlighted infrastructure vulnerabilities (CISA, 2024)
2. **energy infrastructure**:
    - power grids remain attractive targets due to heavy technology dependence
    - renewable energy transition introduces new vulnerabilities if security isn't foundational
3. **communications infrastructure**:
    - 124 cyber operations against Space sector, including the commercial sector, recorded in Ukraine conflict context
    - undersea cable vulnerabilities in Baltic Sea incidents
    - satellite networks and telecommunications increasingly targeted.

The report identifies six compounding complexity factors affecting critical infrastructure:

- geopolitical tensions (60% of organisations report strategy impacts)
- cybercrime sophistication
- AI and emerging technology risks
- regulatory fragmentation
- supply chain interdependencies
- cyber skills gap.

The World Economic Forum's Global Cybersecurity Outlook (2026), just released at the time of the authoring of this report, examines how accelerating AI adoption, geopolitical fragmentation, and widening cyber inequity are reshaping the global risk landscape. The report identifies three key trends including that cyber-enabled fraud has overtaken ransomware as the top Chief Executive Officer (CEO) concern (affecting 73% of respondents to their research), AI-related risks are shifting from offensive capabilities to data exposure concerns, and geopolitical tensions are becoming a defining feature of cybersecurity with declining confidence in national preparedness. The report emphasises the need for collaboration, shared intelligence, and public-private cooperation to address these converging threats.

In terms of Australian research, the Australian Strategic Policy Institute (ASPI) a Canberra Think Tank, (ASPI 2025, Shah 2019), is very supportive of the SOCI Act of 2018 and its amendments. They comment that we currently see the convergence of physical and cyber security, emphasising the need for an ‘all-hazards’ approach that recognises:

1. **interconnected threats:** cyber and physical threats increasingly overlap and compound
2. **technology dependencies:** modern critical infrastructure relies on cyber-physical systems; and
3. **cascading impacts:** incidents in one domain rapidly affect others.

They recognise the SOCI Act's explicit inclusion of data storage systems and supply chain hazards in CIRMP requirements addresses growing recognition that:

1. **third-party dependencies**: critical infrastructure increasingly relies on complex vendor ecosystems
2. **data as infrastructure**: business-critical data storage systems are themselves infrastructure; and
3. **vendor risk management:** organisations must assess and manage security throughout supply chains.

However, ASPI research highlights the need for:

1. **board capability development**: creating questioning cultures rather than requiring specific expertise
2. **cross-functional integration:** breaking down silos between Information Technology (IT), OT, physical security, and business units; and
3. **continuous improvement**: moving beyond tick-box compliance to genuine risk management.

Overall, this brief literature review emphasises the need for an all-hazards approach to supply chain security while maintaining a sophisticated technical approach to the security of OT to protect industrial output and economic productivity from interference. Water, Energy and Communications are all called out as sectors of concern during a time of huge geopolitical disruption, the largely unknown, but concerning, impact of emerging technologies such as AI, and the cascading impact of critical infrastructure breaches.

LEGISLATIVE APPROACHES

It is useful to take an international perspective on critical infrastructure protection legislation and compare the SOCI Act (2018) as it stands in January 2026 with similar legislation proposed or legislated by allies.

Table 4: Legislative approaches

EU	Singapore	UK	Canada	Australia
MAIN LEGISLATION				
Two main directives adopted in December 2022: Network and Information Systems (NIS) 2 (cybersecurity) and Critical Entities Resilience (CER) (physical resilience). Both came into force in January 2023. NIS2 updates the original 2016 framework.	*Cybersecurity Act 2018*, operational since August 2018. Governs Critical Information Infrastructure (CII). Strengthened through 2024 amendments.	NIS Regulations 2018 currently in force. UK's Product *Security and Telecommunications Infrastructure Act 2022* focusses on consumer Internet of Things/smart devices and has Telecommunications provision in Part 2 New Cyber Security and Resilience Bill introduced in November 2025, currently in Parliament. Expected to pass in 2026.	Bill C-26 passed Parliament in December 2024 but died when Parliament prorogued in January 2025. Bill C-8 reintroduced June 2025 with nearly identical content. Not yet law.	SOCI Act fully operational. Updated by major amendments in 2021 and 2022.
CURRENT STATUS				
European Union (EU) Member States had until October 17 2024, to implement the directives into national law. Most have completed or are in final stages. Countries like Belgium, Denmark, Greece, Hungary, and Italy finished early. Germany delayed until December 2025. Affects approximately 100,000 entities across the EU.	Fully operational since 2018. The 2024 amendments strengthened enforcement powers. Covers 11 critical sectors. Operates an active licensing system for cybersecurity service providers.	Current NIS Regulations operating. The new Bill passed first reading in November 2025 and second reading on January 6, 2026. Expected to receive Royal Assent in 2026, with implementation phased through secondary legislation.	No law in force yet. Bill C-26 died in January 2025 when Parliament prorogued. Bill C-8 is now going through the legislative process. After passage, regulations must be developed. Timeline uncertain.	Fully operational since 2018. Major amendments implemented 2021-2022 are now active. Covers 11 sectors across 22 asset classes. Annual compliance cycles established.

LEAD AGENCY				
Multi-level system: European Union Agency for Cybersecurity coordinates across the EU. The NIS Cooperation Group brings Member States together. EU-CyCLONe handles crisis coordination. Each Member State has its own competent authorities and cybersecurity teams.	Cyber Security Agency (CSA) of Singapore acts as the central authority. The Commissioner of Cybersecurity designates which entities are critical infrastructure.	Distributed system with over 12 sector-specific regulators. The National Cyber Security Centre (NCSC) serves as the main coordination point. The National Protective Security Authority advises on critical national infrastructure. The proposed Bill will create a new Information Commission.	Public Safety Canada leads overall policy. Individual sector regulators oversee their areas: Office of the Superintendent of Financial Issues for banking, Bank of Canada for payments, plus Ministers for transport, natural resources, and public safety. Communication Security Establishment provides cyber defence support.	The Department oversees the framework. The CISC coordinates implementation. The Australian Cyber Security Centre (ACSC) receives incident reports. Sector-specific regulators maintain their authority. A whole-of-government approach.
WHO GETS DESIGNATED				
Size-based rule: Organisations with more than 50 employees and more than €10 million annual revenue are automatically included. Member States identify which entities meet the criteria. Some entities are always included regardless of size (like domain name system providers and digital trust services).	The Commissioner of Cybersecurity formally designates Critical Information Infrastructure (CII) based on how critical systems are to essential services. Owners are notified when designated.	Competent authorities identify operators of essential services based on three tests: provides an essential service, depends on network/information systems, and an incident would significantly disrupt the service. Digital service providers self-identify. The Bill adds a new 'critical suppliers' category.	The Governor in Council (Cabinet) designates: (1) which services and systems are vital, (2) classes of operators. Designated operators own, control, or operate critical cyber systems. The process hasn't been implemented yet.	The Minister can declare certain assets as SoNS.
OWNERSHIP RULES				
No specific ownership notification required. Foreign investment is reviewed separately under Regulation 2019/452. Supply chain security rules address third-party risks. Individual Member States can add their own requirements.	Less prescriptive about ownership structure. Foreign investment gets scrutinised through the general national security framework. Focus is on ensuring secure service delivery.	No ownership notification under current NIS. The separate *National Security and Investment Act 2021* reviews foreign investment. The new Bill introduces supply chain security requirements.	No general ownership notification requirement. Telecommunications Act amendments allow government to prohibit high-risk suppliers. Focus remains on operational security rather than ownership.	Mandatory notification: Any change in direct interest of 10% or more must be reported within 30 days. Government can impose conditions on or prohibit acquisitions. A register captures all ownership information. The Foreign Investment Review Board scrutinises critical infrastructure acquisitions.

CYBERSECURITY REQUIREMENTS				
Article 21 lists 10 security measures: risk analysis, incident handling, business continuity, supply chain security, encryption, access control, multi-factor authentication, and more. National authorities can add specific technical requirements.	Each CII sector has a Code of Practice setting technical standards. Requirements include regular audits, penetration testing, incident response capabilities, and cybersecurity governance. Regular compliance assessments conducted.	Current NIS requires risk management, incident notification, and security measures proportionate to risk. The new Bill adds enhanced requirements including supply chain risk management, vulnerability disclosure, and managed service provider security.	Proposed requirements: Cyber security programs aligned with international standards. Must include risk management, incident response, and supply chain security. Specific details will be set in regulations after the law passes.	CIRMPs tailored to how critical each asset is. The CIRMP framework integrates cyber with all other hazards. Maturity-based requirements (baseline, enhanced, or advanced levels). Regular compliance reporting required.
INCIDENT REPORTING TIMELINES				
Three-stage process: 24 hours for early warning, 72 hours for initial notification, 1 month for final report. Only significant incidents (those disrupting services) need reporting. Reports go to national cybersecurity teams and competent authorities.	Within 2 hours for incidents affecting CII availability or specified cybersecurity incidents. Detailed follow-up information required within 14 days.	Current NIS: 72 hours for significant incidents. The new Bill proposes enhanced timelines and thresholds to be set in secondary legislation. Reports go to competent authorities and NCSC.	Proposed: Within a reasonable time of becoming aware of an incident. Specific timelines and thresholds will be established in regulations. Reports go to designated authorities.	Significant impact: Report to ACSC within 12 hours. Relevant impact: Report to ACSC within 72 hours.
MAXIMUM PENALTIES				
Essential entities: Up to €10 million or 2% of global annual revenue (whichever is higher). Important entities: Up to €7 million or 1.4% of global revenue. Member States can set even higher penalties.	Individuals: Up to SGD $100,000 fine or 2 years imprisonment. Corporations: Up to SGD $1 million. Repeat violations can result in higher penalties.	Current NIS: Up to £17 million or 4% of turnover. Proposed Bill: up to £17 million or 10% of turnover for the most serious breaches. The new Information Commission would set civil monetary penalties.	Proposed: Up to CAD $10 million for individuals, CAD $15 million for corporations for the most serious offenses. Administrative monetary penalties to be set in regulations.	Civil penalties: Up to AUD $11.1 million (adjusted annually for inflation). Criminal penalties for serious offenses: Up to 200 penalty units or imprisonment. Both civil and criminal penalties can apply to the same conduct.

UNIQUE FEATURES				
Directive model allows Member States flexibility in implementation. Dual framework separating cyber (NIS2) and physical (CER) security. Automatic inclusion based on size thresholds. Direct personal liability for management. Harmonised penalties across the EU. EU-CyCLONe for crisis coordination. Largest scope covering approximately 100,000 entities.	Highly centralised under CSA. Prescriptive technical standards through Codes of Practice. Licensing system for cybersecurity service providers. Formal designation process for CII. Commissioner has emergency powers to take over systems. Focused specifically on cyber infrastructure.	Distributed authority across more than 12 sector regulators. Criticalities process with Critical National Infrastructure (CNI) knowledge base for visualisation. Data centres designated as critical national infrastructure in September 2024. Flexible 'critical suppliers' mechanism. Regulatory evolution post-Brexit. Proportionate, risk-based philosophy.	Still proposed legislation only. Dual approach combining Telecommunications Act amendments with new Canadian Consumer Specialty Penalty Products Association. Focuses on federally regulated sectors initially (4 sectors). Strong government direction powers. No compensation for compliance costs. Extensive government powers over critical systems.	Single unified national framework. All-hazards CIRMP integrating physical and cyber security together. Asset-based designation rather than size thresholds. Mandatory ownership transparency through the register. Government has last-resort intervention powers to directly control assets. Maturity-based cyber requirements. Two-tier incident reporting (public and confidential).

KEY FINDINGS

Implementation status

Australia and Singapore have the most mature frameworks, both operational since 2018 with established compliance cycles and active enforcement. The UK is operating mostly under its 2018 NIS framework while preparing for major expansion through new legislation expected in 2026 with some Telecommunications legislation available in the *Product Security and Telecommunications Infrastructure Act of 2022*. The EU is actively implementing with most Member States having met or nearing the October 2024 deadline of the original NIS framework. Canada is still in the legislative process with no law in force yet.

How they are organised

Singapore uses the most centralised model with the CSA holding comprehensive authority. Australia combines centralised Commonwealth oversight with coordinated sector regulators. The EU operates through multi-level governance across 27 member states. The UK maintains a distributed model with sector-specific authorities. Canada proposes sector-specific ministerial oversight.

Who and what is covered

The EU uses size-based automatic inclusion (more than 50 employees, more than €10 million revenue) covering approximately 100,000 entities - by far the broadest scope. Australia and Singapore assess infrastructure criticality regardless of size. The UK combines both size and criticality. Canada proposes designating entire classes of operators within sectors.

Cyber vs physical security

Australia stands out by integrating cyber and physical security in a single all-hazards framework through CIRMP. The EU keeps them separate with NIS2 for cyber and CER for physical. Singapore, UK, and Canada focus primarily on cybersecurity, with physical security either implicit or handled through other mechanisms.

Ownership transparency

Australia is unique in requiring ownership notification (more than 10% interest must be reported within 30 days) and maintaining a Register of Critical Infrastructure Assets. No other jurisdiction has comparable ownership transparency requirements—they focus on operational security instead.

Management accountability

The EU is the only jurisdiction with explicit, severe personal liability for management, including potential leadership bans and direct personal accountability. Other jurisdictions rely on general corporate governance duties with limited personal liability provisions.

Government Intervention Powers

Australia and Singapore have the strongest intervention powers, including last-resort authority to directly control or take over assets. Canada proposes strong direction powers. The EU and UK focus more on supervisory enforcement and compliance monitoring.

Financial penalties

The EU has the highest potential penalties at €10 million or 2% of global revenue for essential entities. The UK's proposed Bill sets penalties at £17 million or 10% of turnover. Australia caps civil penalties at AUD $11.1 million. Canada proposes CAD $10-15 million. Singapore has the lowest at SGD $1 million for corporations.

International cooperation

Australia, UK, and Canada are founding members of the Critical 5 forum alongside the United States and New Zealand. Singapore cooperates with Five-Eyes intelligence partners while pursuing Association of Southeast Asian Nations regional integration. The EU serves as a global regulatory model with extraterritorial influence.

UK's social cohesion approach to critical infrastructure: The UK has evolved beyond purely technical infrastructure protection to explicitly recognise social cohesion as equally critical to national security as physical infrastructure itself. Social cohesion is now identified as a 'centre of gravity'; that, if disrupted, significantly weakens national resilience. The key elements of their framework include:

- **interconnected vulnerability** recognising that infrastructure failures disproportionately affect marginalised communities, and that disruption to critical infrastructure can cascade into erosion of social cohesion (e.g. energy grid failures affecting population centres)
- **hybrid threat recognition** and being aware that adversaries deliberately target social cohesion through disinformation, cyber-attacks, as well as sabotage of physical infrastructure. Protecting infrastructure without protecting social cohesion leaves exploitable vulnerabilities
- **whole-of-society resilience** means that infrastructure must be 'socially responsive', not just technically robust, with explicit focus on supporting vulnerable populations during crises and addressing inequitable impacts such as energy poverty and infrastructure inequality in low-income areas.

A major UK initiative was the Building Resilient Communities Report (2024) which identifies social cohesion as the foundation of resilience, calling for it to be prioritised as national policy and embedded in infrastructure planning. While conceptually sophisticated, this social cohesion perspective exists primarily at strategic/policy level rather than embedded in specific cyber security and CNI protection legislation, which remain technically focused. However, this holistic approach places the UK ahead of other nations (Australia, EU, Singapore, Canada) whose frameworks focus on technical and physical resilience without explicit social cohesion integration.

CHAPTER THREE

STAKEHOLDER REVIEW OF THE SOCI ACT

INTRODUCTION

This chapter presents the findings from comprehensive stakeholder engagement undertaken to understand the perspectives of industry and private organisations subject to the SOCI Act. The engagement was designed to address the core questions in the terms of reference, examining whether the SOCI Act is:

- achieving its intended objectives
- functioning as intended
- having any unintended consequences. If so, what are they?

I have also chosen to ask a question regarding the SOCI Act's ability to deal with emergent threats given the speed of development of new technology and the multiple times the SOCI Act has already been modified. To answer these questions, a multi-method approach was employed following an initial literature review. The engagement strategy comprised four complementary streams designed to capture diverse perspectives and ensure comprehensive coverage.

ENGAGEMENT METHODOLOGY

An initial literature review examined international harmonisation with allies' critical infrastructure legislation and approaches. This comparative analysis informed the development of engagement activities across four streams:

- virtual sector roundtables
- consultation meetings
- surveys
- written public submissions.

Each stream is described below, followed by detailed findings from the written submissions, survey results, and roundtable discussions.

Written submissions

As described in Appendix B, written submissions were requested from industry and specifically targeting consultants, lawyers, the cyber security sector and industry players. Invitations were also provided to all TISN members, to selected private sector organisations, the Resilience Expert Advisory Group (REAG) and the Supply Chain Expert Advisory Group (SCEAG). An option for confidential or anonymised submissions was provided.

The written submissions process sought points of view from the public, governments and industry on the three questions listed above.

This allowed for structured arguments from involved industry and government participants, encouraging the contribution of unique perspectives, evidence and recommendations, thereby assisting the Independent Reviewer to develop well-informed recommendations to government. This diversity further enabled fairness and equity of views, heard not just from government stakeholders, and supported a detailed examination of facts, expert evidence and complex issues around the SOCI Act that would have been difficult to manage solely through verbal consultations. A further analysis was also undertaken across all submissions to distil the common themes. A list of public submissions is at Attachment F.

Virtual sector roundtables with accompanying survey

A series of sector-specific roundtables were conducted with the TISN. These were organised into key groups, allowing for additional focussed discussion to extract key issues and concepts related to specific sectors or interests. Stakeholders were identified by the Department, in collaboration with the Independent Reviewer, and

mapped according to sector. For the larger cohorts (up to 500), discussion was one way supported by Mentimeter software to display questions and encourage written feedback and generate word clouds by participants. Sector members were also invited to complete an online survey with a shorter set of questions to allow collection of good quality qualitative data.

Targeted interviews/consultation meetings with accompanying survey

A series of one-on-one and/or small group interviews (virtual or in-person) with government agencies and international partners were conducted to discuss equities and perspectives on the operation of the SOCI Act. This allowed for non-minuted discussion to gather deep insights, implementation challenges and proposed improvements. These discussions were particularly useful in identifying real-life experiences in operating under the SOCI Act and examples of how the SOCI Act could be refined for better use. On occasion, government stakeholders were invited to participate in the survey to further enable the capturing of non-classified insights and proposed improvements for later analysis.

WRITTEN SUBMISSIONS

The independent review received 50 submissions from industry, government, and civil society stakeholders. These submissions affirm the SOCI Act's importance in strengthening Australia's critical infrastructure security and resilience. While the SOCI Act framework has delivered significant improvements in asset visibility, governance, and incident reporting, stakeholders identify key challenges and opportunities for reform to ensure the regime remains effective in a rapidly evolving threat environment.

The thematic analysis of the 50 submissions is presented in Appendix L, examining ten key areas where stakeholders expressed consistent views, areas of contention, or calls for reform. This analysis synthesises the main arguments, identifies patterns of consensus and divergence, and provides representative examples from specific submissions.

KEY FINDINGS FROM WRITTEN SUBMISSIONS

Having examined the detailed thematic analysis of submissions, the following sections synthesises the overarching findings that emerged across all 50 submissions. These key findings, areas of consensus, and points of tension provide a comprehensive summary of stakeholder perspectives on the SOCI Act.

The table below shows how public submissions considered the questions underpinning the review regarding whether the SOCI Act is:

1. achieving its intended objectives
2. functioning as intended
3. having any unintended consequences
4. able to deal with threats from emergent technologies.

Table 5: Key points from public submissions

Theme	Key points made in public submissions	Consensus direction
1) Scope and coverage	**Expand coverage of the SOCI Act** to include all AI infrastructure and services including all offshore dependencies, data poisoning, agentic AI, all content delivery networks (CDN) and satellite and satellite dependencies.	It is necessary to expand SOCI Act with tailored, sector-appropriate rules and with explicit coverage for AI, CDN, space, drones, critical information

	The issue of drones and enterprise detection and response obligations was also raised.	and communications technology storage and other facilities.
2) Regulatory harmonisation and audit duplication	**Reduce duplication of effort in national security activity** with integration and re-use of documentation developed for information security registered assessors program/ISO/Defence Industry Security Program evidence: • harmonise SOCI Act rules and documentation with prudential/sector frameworks and align with global standards such as principles for financial market infrastructures where appropriate for risk management • using these suggestions, develop a 'report once' incident framework with a single portal approach.	Near-unanimous call to rationalise reporting and audits. A need expressed to clarify SOCI integration with: • APRA • ASIC • Reserve Bank of Australia (RBA) • Hosting Certification Framework (HCF) • TSSR • CPS 234
3) Guidance, Definitions and operability	**Need clearer guidance,** such as those provided by ASIC in their regulatory guides, with worked examples: • clear definitions for issues such as critical workers and their access to systems is needed • CIRMP needs practical improvements to make it useful to those who have to operate under it including a need for plain-language materials and templates • Realistic case studies and support with use cases for those who feel burdened by this aspect of compliance.	Consensus was reached on the need for clear definitions and threshold: • CIRMP templates need improvement so as to make them useable • security education was seen as a missing enabler to compliance.
4) Essential Eight (E8) and baselines	The E8 was seen as common minimum with tailoring/equivalence required in some contexts. It was felt that it was necessary to re-evaluate E8 Maturity Level 1 for modern threats.	Agreement on baseline and sector overlays and outcome-based assurance to be suitable across industries. It was noted that a one-size E8 was not necessarily suitable for Telecommunications and OT contexts.
5) Incident reporting and Government Assistance	**Improve reporting** to include near-miss and business continuity activations with clear thresholds: • adopt a 'report once' model across frameworks as noted above • instigate post-incident reviews for government assistance.	As above: • streamline reporting (less duplication, more intelligence value) • provide oversight/transparency for exceptional powers.

	• as above, adopt and align with international best practice.	
6) Supply chain risk	**Two competing models** were presented in submissions: • the first was that of shared uplift with legal responsibility on suppliers • the second was owner-led risk with standard carve-outs and clear guidance.	It is possible that a middle path is established with SOCI Act setting minimum supplier security obligations and consistent contract templates.
7) Sector-specific insights	**Water**: sector-specific rules, national resilience strategy, funding. **Energy**: clean energy vulnerabilities; tech pace. **Telecommunications**: subsea cable protections; clarity on suitable of usage of E8. **Financial**: mature oversight; harmonise for value. **Health**: uneven thresholds; resource constraints; templates needed. **Rail**: vandalism as critical infrastructure attacks; realistic exercises.	Tailored sector approaches while maintaining common baseline standards is best compromise.
8) Education, capability and intelligence	**Capability as a bottleneck across the critical infrastructure sectors was widely expressed** and it was noted that **protective security education** is missing. It was also suggested that mandatory, structured **Cyber Threat Intelligence** (CTI) sharing is needed along with benchmarking tools with AI and analytics. It was also noted that independent quality assurance is needed as well as the establishment of workforce learning pathways.	High level of consensus on education, intelligence and benchmarking as critical enablers for operators. The majority favour mandatory CTI sharing.
9) Timelines and regulatory posture	**Acceleration of reforms** was widely agreed with suggestions that CIRMP rules and changes in reporting should be improved by June 2026. Some felt that assurance should be strengthened sooner with a move from compliance to effectiveness-based audits.	There was common consensus on the need to tighten assurance with mixed views on implementation speed given capacity constraints.

VIRTUAL SECTOR ROUNDTABLES WITH ACCOMPANYING SURVEY

While written submissions provided detailed, structured arguments, the virtual sector roundtables and accompanying surveys captured real-time stakeholder sentiment and enabled broader participation. The following section presents findings from over 600 participants who engaged through Town Halls, sector-specific meetings, and online surveys.

Large groups were surveyed in real-time using Mentimeter voting software, while all participants were offered access to a more detailed Qualtrics survey for deeper personal insights. Survey questions are listed in the appendices.

KEY FINDINGS FROM TOWN HALL AND ROUNDTABLES

Complete sets of questions and results from Mentimeter are displayed graphically and as word clouds in Appendix H. A summary of questions asked which prompted further discussion included:

- is the SOCI Act equipped to deal with emerging threats?
- do current asset classes allow future identification of new classes?
- does the SOCI Act support resilience of critical infrastructure?
- what are the main areas for improvement?
- are the obligations in the SOCI Act clear?
- suggestions to improve specific obligations
- have you experienced issues with definitions?
- which definitions cause issues and suggested improvements
- are penalties for non-compliance effective/adequate?

Based on the Mentimeter consultation results from more than 460 attendees, the SOCI Act consultation reveals a concerning picture with some areas of qualified optimism. The following word cloud typifies some of the responses to questions regarding attitudes towards the SOCI Act.

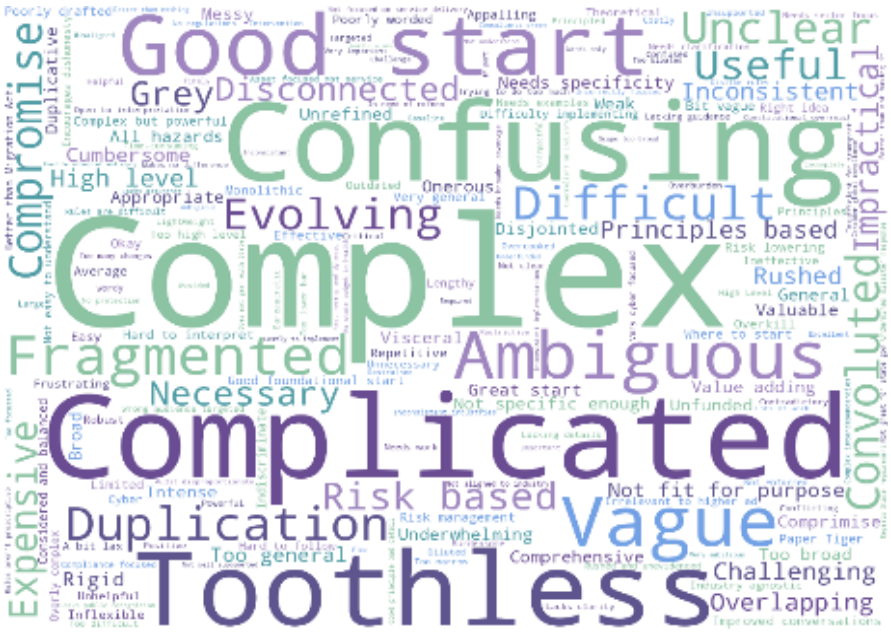


Figure 3: Answer to: From your experiences interacting with SOCI legislation, in one or two words how would you describe the SOCI Act and subordinate legislation?'

As can be seen in Appendix H, the feedback is predominantly critical, with approximately 70% of sentiment towards the SOCI Act being negative. Many respondents used concepts of complexity such as 'complex', 'complicated', and 'confusing', as their dominant descriptors across all sectors. Over half of respondents (118 out of 230) find the obligations unclear, and there's near-universal agreement that definitions are problematic, with 177 out of 217 respondents identifying issues. Terms like 'critical worker', 'protected information', and 'asset versus infrastructure' are seen as ambiguous and inconsistent.

However, in discussion, it did not appear that there was any real philosophical disagreement with the need for the SOCI Act, and there was no suggestion that the Department did anything other than offer support and education. It was also seen as responsive and agile in meeting and offering solutions to issues that respondents did find complicated. There was a warmth towards the Department that is not displayed in the results attained here.

One major issue that I noted too was that respondents were not at all personally analytical of the need to protect Australian critical infrastructure and did not see that compliance with the SOCI Act was the price to pay for protecting this infrastructure. The majority of those who are deeply immersed in the issue of compliance with the SOCI Act do not seem to have an emotional connection to defending and protecting Australia and its citizens. The exceptions to this came from those whose background was Defence and intelligence. This issue is worthy of examination by the Department.

Chapter 2, where international legislation is examined, details the fairly well-known UK perspective of taking a social cohesion lens to critical infrastructure protection and this could be considered in Australia too. We can note that the Australian government has tried to deal with the issue of energy poverty in an era of transition to renewables and it might be possible to harness some of this impetus to encourage a transition.

There are some constructive elements worth noting. A small minority (around 10%) described the SOCI Act positively as 'risk-based,' 'a good start,' or 'evolving,' suggesting some see potential in its foundational approach (see Appendix H). Respondents provided detailed, thoughtful suggestions for improvement, indicating genuine engagement rather than dismissal. The top priorities include simplification, sector-specific guidance, clearer definitions, practical templates and examples, reduced duplication, stronger physical security standards, better funding support, and improved accountability mechanisms.

Stakeholders appear to want the SOCI Act to succeed, and these results show a call for it to move from being compliance-driven to outcome-driven, with real security uplift as the goal. The breadth of feedback across sectors (energy, government, transport, health, water, and others) shows widespread investment in supporting its development, and there is appetite for international alignment with standards like ISO and NIST and harmonisation with international industry partners and governments.

The perception that the Act is 'toothless' is pervasive. When asked if penalties are effective, the overwhelming majority said no, with comments like; 'what penalties?', 'not enforced', and 'easier to pay a fine than comply.' This lack of enforcement appears to have bred cynicism among employees, with stakeholders noting that boards simply do not care about compliance.

In my experience of over twenty years, this attitude towards boards and their lack of care has always existed among critical infrastructure employees. Australia has always taken a position of encouraging boards towards compliance rather than applying penalties. It does appear that a wide range of participants with very varied roles in the critical infrastructure sector is asking for explicit regulation and the application of penalties for non-compliance.

Many respondents do not believe the SOCI Act is equipped to handle emerging threats. They see it as too reactive, too slow compared to evolving risks, and overly focused on cyber security while neglecting physical and personnel security. The legislation is also criticised for duplication and fragmentation, overlapping with other Acts like the *Telecommunications Act 1997*, PSPF and various state rules, without proper integration.

There is wide belief internationally, as well as in the research underpinning this review, that it is currently, and in the foreseeable future, going to be very difficult to manage physical security in an era of AI, quantum and drones. This issue though does point to at least the restructure of the SOCI Act as it now stands, separating legislation and rules and providing a handbook (or guidebook) so as to have a SOCI Act with a minimal and generic legislation, simple dynamic rules and contextual guidance on each new asset class, and the means by which all-hazards risks to the asset may be handled.

Thus, while the SOCI Act started with good intentions, its execution, as viewed by a large town hall meeting and various TISN leaders, has created more confusion than clarity, and without serious restructure of how the legislation is presented and some simplification to its operation, the development of enforcement mechanisms, and practical guidance, it risks remaining ineffective in a time of growing geopolitical disruption and, as presented in a modern literature review in Chapter 2, may struggle to deal with the risks of cyber breach of critical infrastructure and development in :

- **interconnected threats:** cyber and physical threats increasingly overlap and compound
- **technology dependencies:** modern critical infrastructure relies on cyber-physical systems
- **cascading impacts:** incidents in one domain rapidly affect others.

CONSOLIDATION OF SURVEY RESULTS

Detailed survey results are presented in Appendix I. Surveys were offered to the TISN Townhall, REAG, SCEAG, TISN Government and TISN Leadership cohorts who had taken part in Mentimeter survey and discussion so as to develop a richer picture of opinions held. A total of 89 people responded. However, some questions were not mandatory for participants to answer, and therefore the responses are not indicative of the full cohort of respondents. Questions asked were as follows, and parallel those in the Mentimeter survey (above) with opportunity given to supply a more detailed answer.

Table 6: Survey Questions

Survey questions
Section 1: Achievement of Intended Objectives
1. To what extent has the SOCI Act improved the security and resilience of your organisation's critical infrastructure?
2. In your view, what elements of the SOCI Act have been the most effective in meeting its intended objectives?
3. In your view, which aspects of the SOCI Act have been the most challenging to implement for your organisation?
4. Has your organisation experienced any operational or administrative challenges complying with the SOCI Act?
Section 2: Functioning of the Act in Practice
5. Does subsection 12F(3) of the SOCI Act clearly explain the requirement to notify data storage or processing providers?
6. Asset register requirements are clear and practical to implement?
7. Critical Infrastructure Risk Management Program requirements are clear and practical to implement?
8. Telecommunications Security and Risk Management Program requirements are clear and practical to implement?
9. Mandatory Cyber Incident Reporting thresholds are reasonable and achievable?
10. The Enhanced Cyber Security Obligations (ESCO), if applicable to your organisation, are proportionate and practicable?
11. The SOCI Act has increased executive and board focus on critical infrastructure security?
12. How effective is the SOCI Act in addressing current cyber threat environments?

13. How effective is the SOCI Act in addressing current natural hazard and physical threat environments?
14. How effective is the SOCI Act in addressing current supply chain threat environments?
15. How effective is the SOCI Act in addressing current personnel threat environments?

Section 3: Unintended Consequences and Emerging Threats

16. Has the SOCI Act resulted in any unintended impacts or consequences for your organisation (e.g. duplication, delays, burden)?
17. Are there regulatory areas where duplication or overlap occurs (e.g. privacy, APRA CPS 230)?
18. The SOCI Act has resulted in higher compliance costs than expected?
19. The SOCI Act has introduced uncertainty or confusion around allocation of risk and responsibilities?
20. How effective is the SOCI Act's framework in supporting continuous improvement and uplift in critical infrastructure security?
21. What are the main improvements you would recommend to ensure the SOCI Act remains fit-for-purpose?
22. What additional guidance, tools or support would assist compliance?

KEY FINDINGS FROM SURVEY

As with the Mentimeter results, many entities feel the SOCI Act raised awareness and improved governance but also introduced complexity.

Top 5 common themes (ranked in order of frequency):

- **Costs of resourcing /administrative burden:** respondents most frequently raised the time, effort, staffing and funding required to comply with the SOCI Act (e.g. heavier admin load, resource strain) suggesting that, for example, reporting requirements are driving *'increased administrative costs'*
- **Incident reporting thresholds and timeframes (12/72 hours):** there was a common focus on whether the time windows for reporting under the SOCI Act are workable, plus ambiguity about when the clock starts ('becoming aware') and sector suitability. One comment suggested that "*Time periods should be specific to the sector… the definition for 'becoming aware' needs to be clarified"*
- **Harmonisation with other frameworks (APRA, Privacy, DISP/PSPF):** strong calls were made to reduce duplication by mapping/aligning SOCI Act obligations with existing regulatory and assurance frameworks (APRA CPS 230/234, Privacy Act, DISP, PSPF)
- **Clarity required in the definitions (ambiguity, vagueness, sector fit):** many responses emphasised unclear definitions, broad language, and inconsistent interpretation across sectors which was making compliance harder and potentially risky in a crisis
- **Duplication and overlap (parallel obligations, double reporting):** respondents described duplicated reporting and overlapping obligations across Commonwealth/state regimes and other sector regulations which were adding friction and cost.

Other trends:

- **Security and resilience uplift is mostly seen as 'moderate'**: 41.5% said the SOCI Act has 'moderately' improved security/resilience while a further 23.1% reported 'slightly'. 16.9% said it did not improve security or resilience at all
- **Administrative burden is widespread**: 68.3% have experienced operational/administrative challenges complying with the SOCI Act
- **Clarity is mixed regarding CIRMP requirements**: CIRMP requirements are clear 'in part' for most respondents (45.3%)
- **Incident reporting thresholds are largely seen as reasonable**: 78.5% agree, although some comments highlight timing and definition issues

- **The SOCI Act's effectiveness varies by threat domain**: most rate the SOCI Act as 'moderately/partially effective' across cyber, natural/physical, supply chain, and personnel threats - with few 'very effective' ratings
- **Duplication and cost pressures are common**: 55.6% report regulatory overlap while 58.9% say compliance costs are higher than expected in Question 18.

GOVERNMENT STAKEHOLDER REVIEW OF THE SOCI ACT

There was broad federal government stakeholder engagement undertaken to understand the perspectives of those involved with national security implications and governance within their own department. The engagement was designed to address the core questions in the terms of reference, examining whether the SOCI Act is:

- achieving its intended objectives
- functioning as intended
- having any unintended consequences. If so, what are they?

I have also chosen to ask a question regarding the SOCI Act's ability to deal with emergent threats given the speed of development of new technology and the multiple times the SOCI Act has already been modified.

PROPOSED AMENDMENTS TO THE CRITICAL INFRASTRUCTURE RISK MANAGEMENT PROGRAM (CIRMP) RULES AS GOVERNMENT STAKEHOLDER INPUT

During the time that this independent review has been underway in November and December 2025 and January 2026, a new consultation paper, *Consultation Paper: Proposed amendments to enhance the Critical Infrastructure Risk Management Program (CIRMP) Rules* has been released by the Department and assesses more proposed reforms in the context of the SOCI Act as amended to 2025. In this section, I describe these proposed amendments and include them as the Department's input to the independent review and examine the anticipated effects of the proposed amendments on the operation and maturity of:

- the SOCI Act framework
- SOCI Act compliance
- impacts for affected industry sectors
- the overall protection and resilience of Australia's critical infrastructure system.

IMPACT OF PROPOSED AMENDMENTS

Overall, the proposed amendments represent a significant and largely positive evolution of the CIRMP framework. They do not alter the primary legislative architecture of the SOCI Act but materially strengthen its operation by deepening obligations under Part 2A through subordinate rules. In practice, the reforms shift CIRMP from a baseline, principles-based risk management requirement toward a more intelligence-informed and semi-prescriptive security uplift for higher-risk asset classes.

The reforms can be understood as a transition from *risk awareness* to *demonstrable risk treatment*. They introduce clearer expectations, stronger governance signals, and more consistent minimum practices across sectors that are increasingly targeted by sophisticated state-sponsored and criminal threat actors.

The proposed amendments are likely to impose **moderate to high compliance and cost impacts**, concentrated in cyber-physical and highly interconnected sectors. Key impacts include an increased compliance workload, including the development and maintenance of new artefacts such as personnel security plans, supply-chain maps, vendor risk assessments, and cyber uplift roadmaps. There will also be a need for capital investment in cyber controls, identity and access management, network architecture, and monitoring capabilities and some operational costs associated with supplier reassessment, logging and monitoring, background checking, training, and audit.

Positively speaking, there will be greater board and executive accountability for security outcomes, driven by formal attestation requirements and increased regulatory scrutiny. Several risks may affect the successful implementation of the reforms including shortages in specialist skills, particularly in OT security, identity engineering, and supply-chain risk management and a need to avoid compliance driven by artefact production rather than risk reduction, particularly in the early years of implementation. Smaller or regionally critical operators with limited internal security capability will need support and guidance.

PROPOSED AMENDMENT FROM WRITTEN SUBMISSIONS

Several written submissions from federal government departments were received and input from minuted meetings was also considered. These are summarised here:

Key strengths of the SOCI Act identified:

The SOCI Act is a principles-based framework allowing organisational flexibility but making known, in a very clear way, the critical infrastructure obligations of an entity. By taking an all-hazards approach it has recognised risks, beyond those of cybersecurity, that need to be managed and recognises Australia's unique features of a relatively small number of key economic players and our infrastructure interconnectedness. While the SOCI Act has made Australia a global leader in critical infrastructure security, the framework needs updates to address modern threats, complex corporate structures, and emerging technologies.

Major concepts discussed include:

- **Definitions**: expand and clarify asset classifications to prevent regulatory gaps, including covering entire corporate groups rather than parts of such groups which allows for avoidance, adding space assets since there is much growth and dependence on space assets for the supply of communications services, updating energy definitions and thresholds for distributed markets, and expanding healthcare and food supply chain protections by additions and alternative methods of approach
- **Register**: improve data quality and real-time information sharing across regulatory authorities to better understand infrastructure interdependencies
- **Mandate** government information sharing with operators (similar to US CISA 2015) and insist on bidirectional information exchange between government agencies and critical infrastructure operators about cybersecurity threats, vulnerabilities, and incidents
- **Risk management programs:** add flexibility for urgent vulnerability patching, extend background checks to all assets, require annual reviews, and create whistleblower protections
- **Cyber incident reporting:** expand to 'all-hazards' reporting including technical outages, and ensure offshore operations meet same standards
- **TISN compliance:** recognise voluntary collaboration as part of TISN as a mitigating factor in enforcement actions

- **SoNS:** streamline declaration processes, expand to all-hazards approach, improve operationalisation and temporary declaration as a SoNS
- **Ministerial Directions**: lower thresholds for government intervention before risks materialise, add powers to address infrastructure (not just personnel) risks
- **Assets under construction**: extend protections to infrastructure during development
- **High risk vendors**: create powers to ban certain technologies or suppliers posing extreme risks
- **Information sharing**: clarify Part 4 to facilitate best practice sharing while protecting sensitive information.

AREAS OF STRONG GOVERNMENT STAKEHOLDER CONSENSUS

Key areas of discussion included a range of topics:

1. **All sectors**: Issues relating to foreign ownership were raised by many stakeholders, with some identifying potential national security risks as a result. Other stakeholders acknowledged that whilst foreign owned entities may present a risk, foreign ownership is not the only vector available to exert foreign influence, with many vectors falling outside direct SOCI Act regulation. Risks associated with FOCI are present across critical infrastructure, commonly in areas such as supply chain, where there is no appropriate domestic alternative. The SOCI Act should be designed to deal with the wide variety of FOCI risks, noting the risk of foreign ownership is predominantly managed through the *Foreign Acquisitions and Takeovers Act 1975*. It should be noted that SOCI-Act regulated entities have a wide range of organisational structures, including large multinationals, foreign owned investments, state owned enterprises, large domestic organisations and small and medium businesses. As a result, many of them are subject to multiple legislative requirements, which must be met prior to operating in the Australian market. Some stakeholder feedback focused on the perception that investment into the Australian market was challenging, given the potentially multiple layers of regulation to move through, with some stakeholders perceiving that there were unequal obligations which prevented their further investment. It appears some of this relates to the perceived lack of compliance action, with entities concerned that whilst they were complying (at a cost to their business) their competitors were not. Per my recommendations, consideration should be given to reducing legislative duplication where possible and increasing compliance action when appropriate.

2. **Energy sector**: another major issue that requires thought is that of the Electricity sub-sector during a time of transition to renewables. The SOCI Act applies to generators larger than 30 Megawatts (MW). Thus it is necessary to amend the SOCI Act to place cyber obligations (e.g. AESCSF as developed by the electricity industry) directly on inverter OEMs. Alternatively, it might be necessary to require transmission networks or generators to report whether and how they pass obligations through the supply chain to OEMs and others. Aggregators and VPP operators are also major attack surfaces and have no obligations under the SOCI Act, even if aggregated generation exceeds 30 MW.

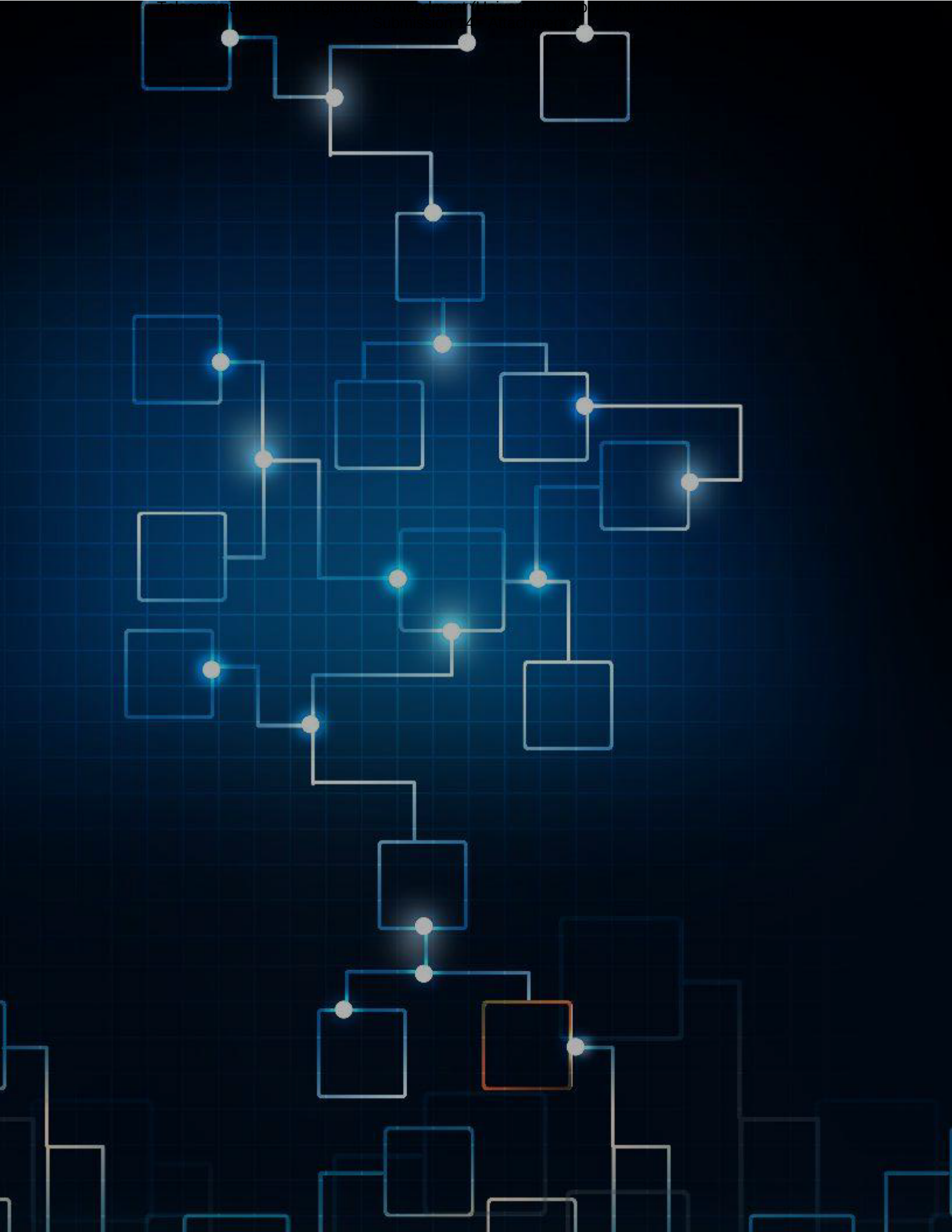
3. **Compliance challenges**: there is tension between a ‘helping hand’ approach versus stricter enforcement given the severity of national security threats.

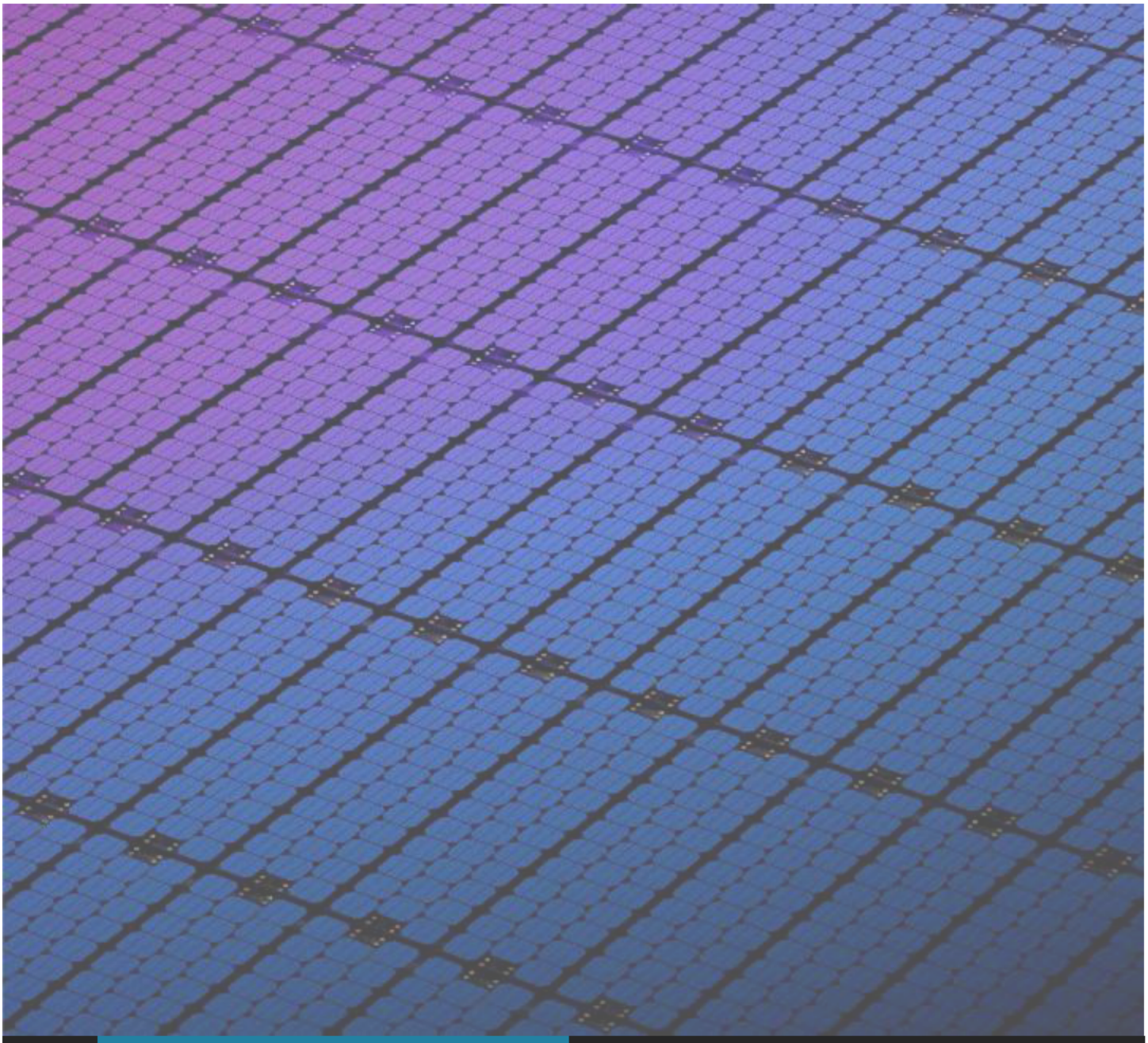
4. **Sector and asset class definitions**: other issues have arisen in debate with TISN groups and individual federal government departments over the breadth of critical infrastructure sectors and asset classes, and the need to enhance and expand both the sectors and asset classes where definitions do not match current context and/or practice. Examples of this include the Higher Education and Research sector and the response of some universities who have concluded that none of their research involves critical infrastructure. This issue is very worrying since universities face foreign interference risks, particularly around research security and the large number of international STEM students. University foreign interference guidelines are now considered static and inconsistently applied and are problematic since they

are voluntary rather than mandated. It might be necessary to consider a new definition of Higher Education and Research to encompass all forms of Higher Educational research and institutions such as CSIRO, NHMRC and other medical research, co-operative research centres and projects and Defence funded research carried out in universities.

5. **Newer sectors**: some critical infrastructure sectors and their asset classes are new or not 'switched on' and so it may be necessary to give deeper thought to, for example, how to redefine Healthcare and Medical as a sector and consider which assets are critical; this might be deeply connected to the medical supply chain and need cross-sector input. Other issues arise with the use of internationally based satellite services across regional and remote Australia. Many critical infrastructure sectors in regional and remote areas rely on such services which are not covered by the SOCI Act.

6. **Self-attestation**: self-attestation by company boards on their risk management programs remains common. Concern was expressed that the approach has not evolved significantly since 2005, with cyber reporting still largely voluntary and ad hoc. There was some acceptance of introducing an appropriately qualified expert into the process to provide external assurance, such as an individual with a chartered cyber engineering qualification or a CP Cyber or an individual at operator level with suitable SOCI Act training at Certificate Level III or equivalent.





CHAPTER FOUR

CONCLUSION AND RECOMMENDATIONS

CONCLUSION

This report has drawn on a literature review and review of international legislation and a comprehensive stakeholder engagement process encompassing 50 written public submissions, surveys from 89 respondents, and interactive roundtables with over 600 participants. It provides a rich and nuanced picture of how the SOCI Act is functioning in practice from an industry perspective. It also draws on at least five submissions from relevant federal government departments, at least ten minuted meetings and many other one-on-one discussions with industry, academia and government.

My overarching conclusion is that the SOCI Act does need major legislative change. This needs to be completed in such a way that permanent change to the SOCI Act is produced without the need for constant modification due to emerging technological change or geopolitical threat. In this was the complexity and confusion that has been identified will be removed. The SOCI Act will need to become agile and responsive, and able to deal with ongoing and expected growth in grey zone warfare, the weaponisation of dual-use technology and the same kind of attacks on our supply chain as those experienced in the EU and the UK. It also needs to include the development of risk management of the infrastructure surrounding the growing use of renewables and satellites and the vulnerability of existing sectors such as Medical and Health Services and Higher Education and Research.

There will always be a cost in answering the call to respond to threats to our Australian critical infrastructure. To do less than completely restructure the SOCI Act at a time of ongoing geophysical and geopolitical disruption, accompanied by all-hazard threats to our infrastructure, would be naïve.

In Chapter 2, a literature review indicated that the need for an all-hazards approach to supply chain security while maintaining a sophisticated technical approach to the security of OT is both necessary and justified. It is important to protect industrial output and economic productivity from interference. Water, energy and communications are all called out as sectors of concern during a time of huge geopolitical disruption, the largely unknown, but concerning, impact of emerging technologies such as AI, and the cascading impact of critical infrastructure breaches.

When examining the legislation of some our closest allies that has developed since 2018, it appears that Australia and Singapore have the most mature frameworks, both operational since 2018 with established compliance cycles and active enforcement. The UK is operating under its 2018 NIS framework with new legislation to be enacted in 2026. The EU is actively implementing change while Canada is still working on its legislation. One positive finding is the holistic approach that places the UK ahead of other nations with a framework that explicitly recognises the role critical infrastructure plays in a cohesive society.

In Chapter 3, stakeholders across all sectors acknowledge that the SOCI Act has successfully elevated critical infrastructure security on corporate and government agendas. Submissions, survey responses, and roundtable discussions consistently note that the SOCI Act has:

- increased executive and board-level awareness of infrastructure vulnerabilities
- established baseline governance frameworks and accountability structures
- improved asset visibility and incident reporting mechanisms
- created a common language for discussing critical infrastructure risks across sectors.

However, this recognition is tempered by significant concerns about implementation complexity, resource burdens, and unintended consequences that may be undermining the SOCI Act's effectiveness.

RECOMMENDATIONS

The issue of duplication emerged as the third most common concern in surveys and featured prominently in submissions and roundtables. Notably, no submission defended the status quo and rather the debate centres on how harmonisation might be obtained rather than whether it is needed. The SOCI Act overlaps substantially with:

- APRA CPS 230 and CPS 234 (operational risk and information security for regulated entities)
- Privacy Act requirements (data breach notification)
- PSPF and DISP
- telecommunication specific legislation; and
- state-level critical infrastructure and emergency management frameworks.

RECOMMENDATION 1

Remove all possible Commonwealth regulatory duplication from the SOCI Act to produce harmonisation and reduce the administrative burden.

An overwhelming majority of town hall respondents characterised penalties as 'toothless,' with common comments including 'what penalties?', 'not enforced', and 'easier to pay a fine than comply'. This perception undermines the SOCI Act's credibility and reduces board-level engagement. When compliance is seen as optional or penalties are viewed as merely a cost of doing business, the regulatory regime struggles to drive genuine security uplift. The current posture is characterised as 'light touch' compliance focused on producing documents rather than demonstrating effective risk management. Stakeholders call for effectiveness-based assurance, post-incident reviews to validate preparedness, and maturity-based tiering that rewards entities with strong security postures rather than treating all obliged entities identically. The lack of visible enforcement action contributes to a compliance-driven rather than outcomes-driven culture.

RECOMMENDATION 2

Move from a 'light touch' compliance approach focus on admin and documentation to that of a penalty-based risk management process with the real enforcement of penalties.

Stakeholders want ASIC-style regulatory guides with worked examples, templates, and plain-language materials. The current guidance is perceived as insufficient, leading to over-reliance on expensive external consultants and inconsistent interpretations. Practical tools such as CIRMP templates, attestation guides and asset register frameworks would significantly reduce compliance burden.

RECOMMENDATION 3

Develop ASIC-style regulatory guides with worked examples, templates, and plain-language materials. Examine international approaches to industry peer committees and guides to support all regulated entities.

When asked whether the SOCI Act is equipped to deal with emerging threats, the majority of roundtable participants responded in the negative. Key concerns include:

- **AI and quantum risks:** AI-enabled attacks, offshore AI dependencies, data poisoning, agentic AI risks, and quantum cryptography vulnerabilities as critical gaps not explicitly addressed by current SOCI Act provisions

- **Physical threat vectors:** unauthorised drones and systemic reliance on space-based services (global positioning systems/position, navigation and timing, satellite communications) introduce vulnerabilities that the SOCI Act does not adequately address
- **Cyber-heavy focus:** stakeholders note that physical security, personnel security, and supply chain resilience receive insufficient attention compared to cyber threats, despite their critical importance to infrastructure protection
- **Legislative agility:** the SOCI Act has already been modified multiple times, yet stakeholders perceive it as too slow to keep pace with rapidly evolving threats. The lack of a hazard-agnostic approach limits flexibility in responding to novel threat vectors.

Written submissions overwhelmingly support expanding coverage to include AI services, CDN, hyperscale cloud providers, space assets, and drone detection/response capabilities. However, this expansion must be accompanied by sector-specific guidance and flexibility to avoid the rigidity that currently hampers implementation.

RECOMMENDATION 4

Home Affairs to work with the TISN community, Australian Signals Directorate (ASD), the Australian Security Intelligence Organisation (ASIO), the National Cyber-Security Co-ordinator, the Department of Industry, Science and Resources (DISR), particularly the Space Agency, and the Department of Foreign Affairs and Trade (DFAT) Cyber Ambassador to respond to concerns on emerging technologies. Home Affairs to lead in examining the impact of AI, quantum, physical threat vectors and the role of Operational Technology (OT) Cybersecurity as they relate to the SOCI Act.

I accept the summary of amendments to the CIRMP rules while advising working toward simplification and rationalisation of the SOCI Act framework to develop a new simpler principles-based SOCI Act. This would have key obligations, offences and penalties, supported by rules to ensure flexibility and futureproofing, and underpinned by detailed thematic handbooks or rulebooks with the prescriptive detail on how to comply.

RECOMMENDATION 5

Enhance TISN capability through education and information sharing.

There is strong support for mandatory cyber threat intelligence sharing, protective security education programs, workforce development initiatives, and structured cross-sector exercises. These capabilities would enable entities to implement SOCI Act requirements more effectively and respond more rapidly to emerging threats.

RECOMMENDATION 6

Accept the summary of amendments to the CIRMP rules while working toward simplification and rationalisation of the SOCI Act framework to develop a new simpler principles-based SOCI Act. This would have key obligations, offences and penalties, supported by rules to ensure flexibility and futureproofing, and underpinned by detailed thematic handbooks or rulebooks with the prescriptive detail on how to comply.

RECOMMENDATION 6A

Issues to examine include:

Definitions: expand what counts as critical infrastructure (corporate groups, space assets, energy systems, healthcare/food supply). Consider whether new sectors or asset classes need to be added or modified.

Register: examine the need for better data quality and real-time sharing between agencies.

Information sharing mandate: require two-way threat information exchange between government and operators.

Risk management programs: allow faster security patches, extend background checks, add annual reviews and whistleblower protections.

Incident reporting: expand to cover all types of outages, include offshore operations.

TISN compliance: credit voluntary cooperation when enforcing penalties.

SoNS: simplify declaration process, cover all hazards, allow temporary declarations of SoNS.

Ministerial Directions: give government earlier intervention powers for infrastructure risks.

Hosting certification: create a legal framework for protecting government data.

Assets under construction: protect infrastructure while it is being built.

High risk vendors: create power to ban dangerous technologies or suppliers.

Information sharing: clarify rules for sharing best practices without exposing sensitive information.

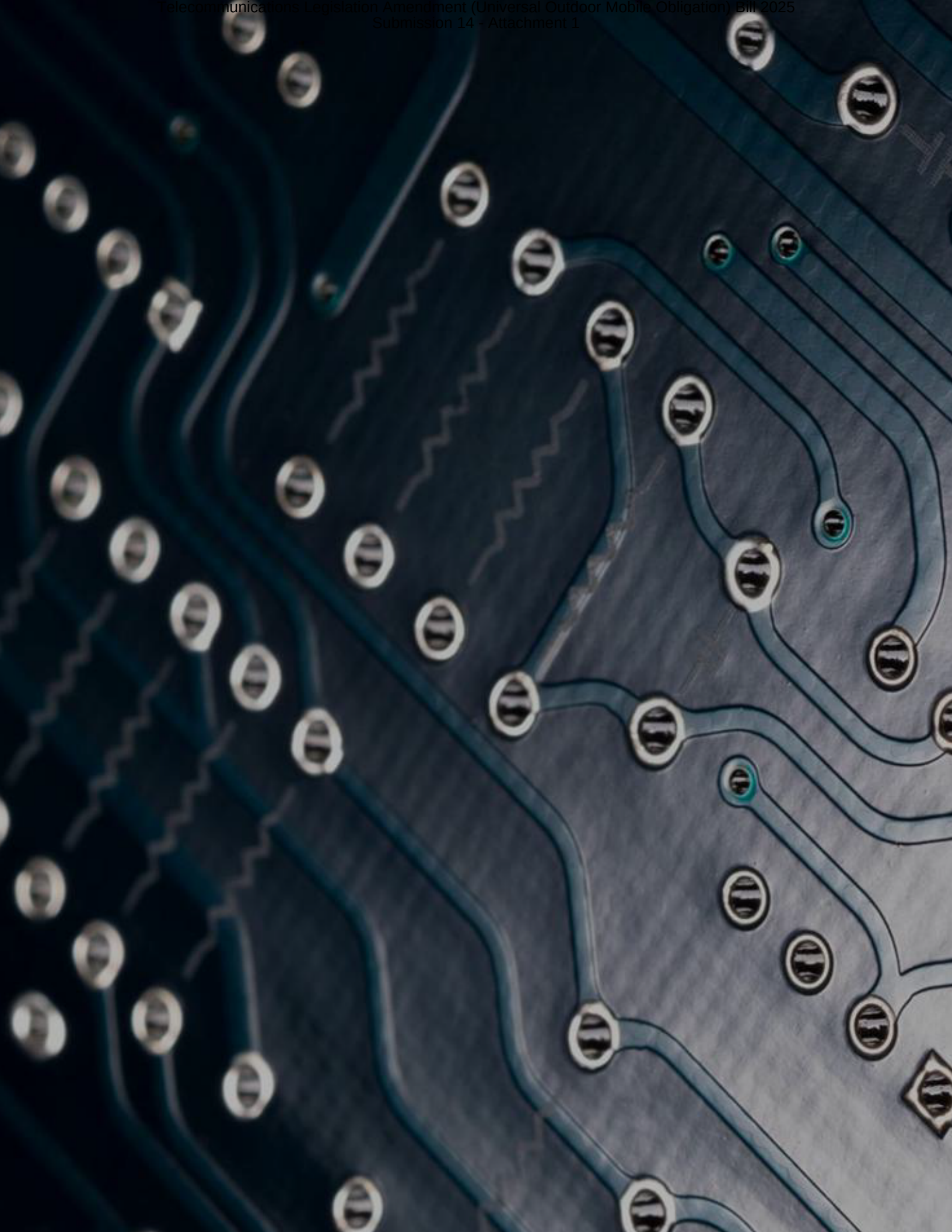
The SOCI Act and other federal legislation: the SOCI Act is effective and useful and should be enhanced and modified to include areas of national security which are currently dealt with by other legislation. The right tools should be used for national security legislation.

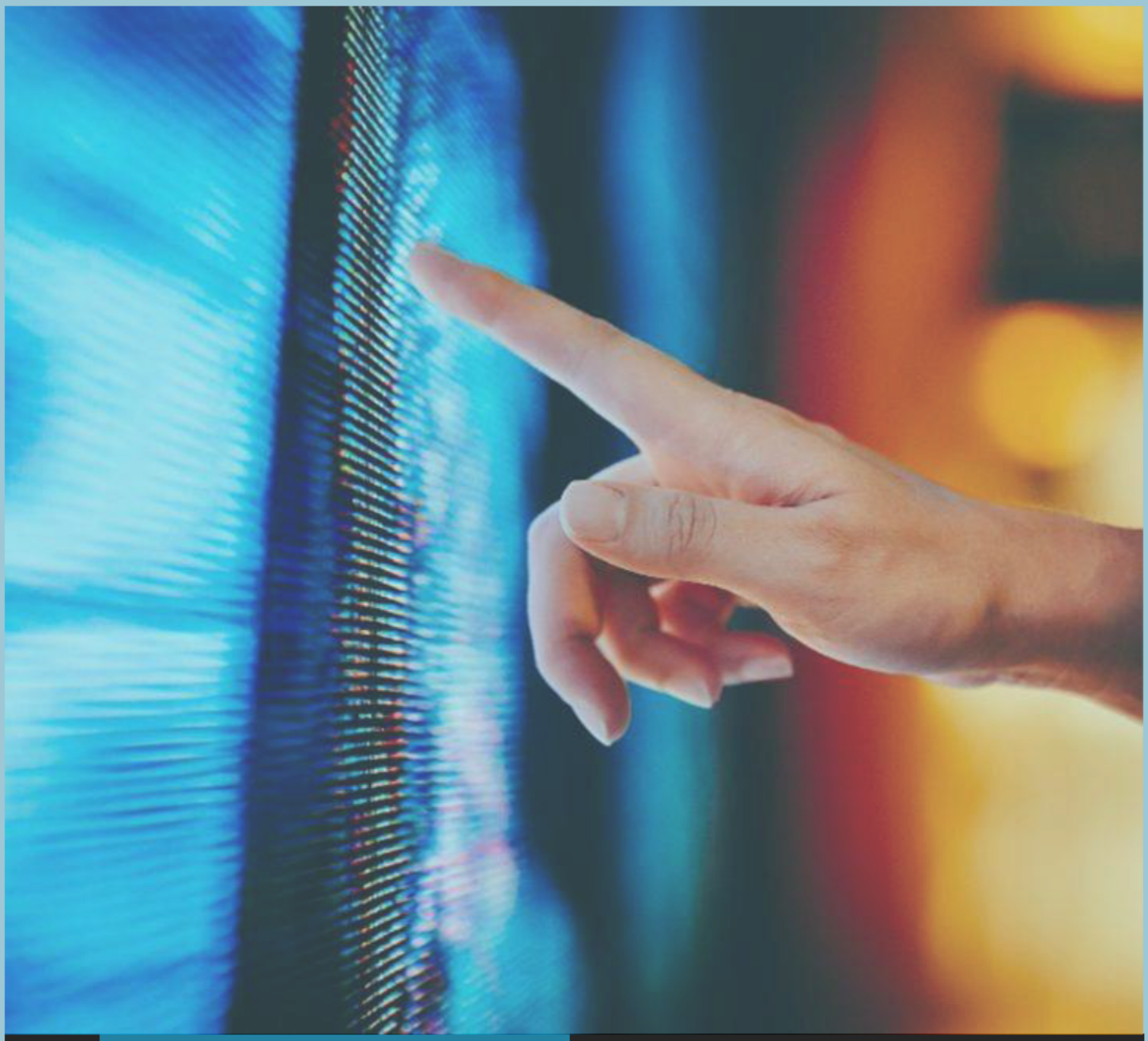
Energy sector: the SOCI Act was designed for traditional energy sources and may not adequately address the energy transition and emerging threats. Major concerns include supply chain risks, with key operational players not being captured by CIRMP requirements despite managing critical operations. Consider issues with generator limits, inverter OEMs and aggregators and VPP operators.

Education sector: consider a new definition of the Higher Education and Research sector to encompass all forms of Higher Education research and the institutions carrying out such research.

National security concerns: examine where, and why, there is limited authority to mandate actions which causes a reactive rather than proactive posture due to non-mandatory reporting, and inability to access critical information needed for threat response.

Self-attestation: consider self-attestation by company boards on their risk management programs which remains common. Consider introducing an appropriately qualified expert into the process to provide external assurance, such as an individual with a chartered cyber engineering qualification or a CP Cyber or an individual at operator level with a suitable SOCI Act training at Cert Level III or equivalent.





APPENDIX A

TERMS OF REFERENCE

TERMS OF REFERENCE FOR THE INDEPENDENT REVIEW OF THE SECURITY OF CRITICAL INFRASTRUCTURE ACT 2018

CONTEXT

The *Security of Critical Infrastructure Act 2018* (SOCI Act) is Australia's key legislative framework for safeguarding the security and resilience of critical infrastructure. Since its commencement, the Act has undergone significant reform, including major amendments in 2021, 2022 and 2024, to respond to a rapidly changing threat landscape. These amendments expanded the Act's coverage to additional sectors, introduced obligations such as mandatory cyber incident reporting, risk management programs, and enhanced cyber security requirements for systems of national significance. The cumulative effect of these successive reforms is a more robust but also more complex regulatory framework for industry and government to navigate.

Section 60A of the SOCI Act requires an independent review be conducted into the 'operation' of the Act. The Minister has agreed with the Parliamentary Joint Committee on Intelligence and Security (PJCIS) to 'initiate' this independent review by 1 November 2025 (already underway) and the Department is aiming to identify the Independent Reviewer and commence the review as soon as possible.

Further, the Department is required to undertake post implementation review obligations stemming from the 2021 and 2022 legislative reforms to the SOCI Act 2018. The Terms of Reference have been developed to address these obligations.

PURPOSE AND SCOPE OF THE REVIEW

The purpose of the review is to assess whether the SOCI Act, as amended, is operating as intended. This is to ensure the legislation is fit for purpose, to identify any problems or gaps and to consider if amendments are needed.

The review will focus on whether the SOCI Act is:

- achieving its intended objectives
- functioning as intended
- having any unintended consequences. If so, what are they?
- the reviewer may also consider other matters that arise in the course of the review that are relevant to the operation of the SOCI Act, in consultation with the Department.

The Final Report should also contain information that addresses the following seven questions, outlined in the Office of Impact Analysis Post Implementation Reviews guidance booklet:

1. What problem was the policy/legislation meant to solve?
2. Why was government action needed?
3. What policy options were considered?
4. What were the impacts of the policy?
5. Which stakeholders have been consulted?
6. Has the regulation delivered a net benefit?
7. How was the policy implemented and evaluated?

Note the review or report does not have to be structured against these seven questions, but the report should present information that addresses them.

CONDUCT OF THE REVIEW

The review will be led by an eminent, independent expert appointed by and reporting to the Minister for Home Affairs. The reviewer will operate at arm's length from Government to ensure independence and impartiality, and will have discretion over the methodology, provided it is consistent with the purpose and scope set out above.

The Department will provide secretariat support to the reviewer.

The reviewer may consult with relevant stakeholders including owners and operators of critical infrastructure assets, peak industry bodies, Commonwealth regulators and policy agencies, state and territory governments, and technical, academic and other subject-matter experts as appropriate.

The reviewer may consider relevant classified material, previous reviews, risk assessments and public submissions where appropriate. Any confidential or sensitive information will be handled in accordance with applicable laws and agreed security protocols.

If the PJCIS initiates a separate review under section 60B during the timeframe of this independent review, efforts should be made to coordinate or share insights as appropriate. The Final Report will be provided to PJCIS.

DELIVERABLES AND TIMING

The review will commence in November 2025. The reviewer will provide a draft report to the Department in January 2026 and a final written report to the Minister for Home Affairs by 2 February 2026 before commencement of the Autumn Parliamentary sittings in 2026. The report will detail the review's findings, conclusions, and recommendations for improving the SOCI Act and its associated framework, against the scope detailed in these Terms of Reference and Statement of Work. Recommendations should be practical, evidence-based, and prioritised. The report should be suitable for public release, although classified annexes may be provided separately where necessary.

Consistent with the SOCI Act, the Minister for Home Affairs must table the Final Report in both Houses of Parliament within 15 sitting days after the report is given to the Minister.

APPENDIX B

RESEARCH PROCESS

RESEARCH PROCESS

All lines of methodology for the independent review were structured around the independent review's terms of reference (refer Appendix A), forming an iterative process as consultations and the review-at -large progressed. Stakeholder engagement was formulated to understand a wide range of views of those in government, industry and private organisations who have obligations under the SOCI legislation. Following a literature review, engagement activities were across four streams: virtual sector roundtables, consultation meetings, surveys, written public submissions.

Literature review

Focused research was undertaken including domestic and international policy research, reviews, white papers and a narrow search of academic literature in critical infrastructure protection and legislation, to inform the critical infrastructure landscape both domestically and internationally. This contributed to the building of foundational knowledge, the identification of gaps in current national security efforts for critical infrastructure protection and to guide key points and questions for the review. This was also important in understanding current concepts, theories and models around critical infrastructure protection and risk management.

The Departmental taskforce (set up to support the independent review) provided a package of documents that were used in the above, including annual reports, legislation, legislative amendments to the SOCI Act, consultation papers, fact sheets, legislative obligations, information on the SOCI Act risk management program and reporting frameworks.

Virtual sector roundtables with accompanying survey

A series of sector-specific roundtables were conducted on the TISN – combined due to time constraints. These were organised into key groups, allowing for additional focussed discussion to extract key issues and concepts related to specific sectors or interests. Stakeholders were identified by the Department, in collaboration with the Independent Reviewer, and mapped according to sector. For the larger cohorts (up to 500), discussion was one way supported by Mentimeter software to display questions and encourage written feedback and generate word clouds by participants.

Sector members were then invited to complete an online survey with a shorter set of questions to allow collection of good quality qualitative data. Survey questions were designed to enable wider engagement and as a supplementary engagement mechanism. Manual qualitative analysis of the survey responses was supported by AI functionality to identify key themes and input.

Targeted interviews/consultation meetings with accompanying survey

A series of one-on-one and/or small group interviews (virtual or in-person) with government agencies and international partners were conducted to discuss equities and perspectives on the operation of the SOCI Act. This allowed for non-minuted discussion to gather deep insights, implementation challenges and proposed improvements. Further, these discussions allowed the incorporation of diverse and also specific perspectives that enhanced the quality, relevance and legitimacy of the review. These discussions were particularly useful in identifying real life experiences in operating under the SOCI Act and examples of how the Act could be refined for better use. This also built trust and transparency for the review, showing genuine intention to understand how the SOCI Act is used nationally and the Government's commitment to bettering users experience and to close the gap between policy and practice.

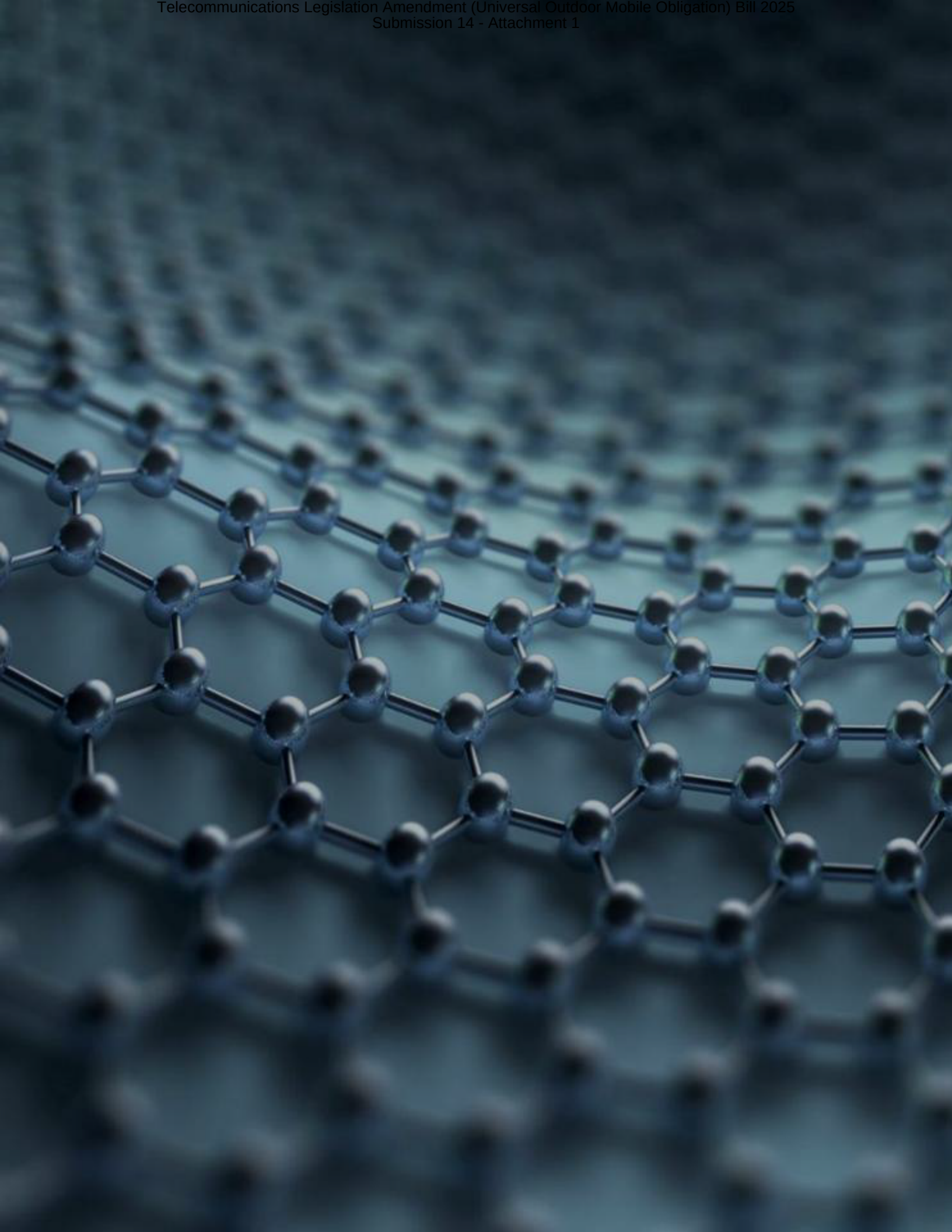
On occasion, government stakeholders were invited to participate in the survey to further enable the capturing of non-classified insights and proposed improvements for later analysis.

Written submissions

An online portal was opened on the Department's website to receive written submissions, specifically targeting consultants, lawyers, the cyber security sector and industry players. Invitations were also provided to all TISN members, to select and known private sector organisations, the REAG and the SCEAG. An option for confidential or anonymised submissions was provided.
The written submissions process sought points of view from the public, governments and industry on three questions:

- is the SOCI Act achieving its intended objectives?
- is the SOCI Act functioning as intended?
- is the SOCI Act having any unintended consequences. If so, what are they?

This allowed for structured arguments from involved industry and government participants, encouraging the contribution of unique perspectives, evidence and recommendations, thereby assisting the Independent Reviewer to develop well informed recommendations to the Government. This diversity further enabled fairness and equity of views, heard not just from government, and supported a detailed examination of facts, expert evidence and complex issues around the SOCI Act that would have been difficult to manage solely through verbal consultations. A further analysis was also undertaken across all submissions to distil the common themes. A list of public submissions is at Attachment F.



APPENDIX C

SURVEY QUESTIONS

Table 7: Survey Questions and Sub-Questions

Pre Survey	Questions
	Which sector does your organisation operate in? What is the size of your organisation? What is your job title?
Section 1: Achievement of Intended Objectives	**Questions**
1	To what extent has the SOCI Act improved the security and resilience of your organisation's critical infrastructure?
2	In your view, what elements of the SOCI Act have been the most effective in meeting its intended objectives?
3	In your view, which aspects of the SOCI Act have been the most challenging to implement for your organisation?
4	Has your organisation experienced any operational or administrative challenges complying with the SOCI Act
4(a)	If you answered 'Yes', please briefly describe
Section 2: Functioning of the Act in Practice	**Questions**
5	Does subsection 12F(3) of the SOCI Act clearly explain the requirement to notify data storage or processing providers? Y/N/In Part
5(a)	If you answered 'In Part' or 'No", please explain your answer.
6	Asset register requirements are clear and practical to implement? Y/N/In Part
6(a)	If you answered 'In Part' or 'No", please explain your answer.
7	Critical Infrastructure Risk Management Program requirements are clear and practical to implement? Y/N/In Part
7(a)	If you answered 'In Part' or 'No", please explain your answer.
8	Telecommunications Security and Risk Management Program requirements are clear and practical to implement? Y/N/In Part
8(a)	If you answered 'In Part' or 'No", please explain your answer.
9	Mandatory cyber incident reporting thresholds are reasonable and achievable? Y/N/In Part
9(a)	If you answered 'In Part' or 'No", please explain your answer.
10	The Enhanced Cyber Security Obligations (ESCO), if applicable to your organisation, are proportionate and practicable? Y/N/In Part
10(a)	If you answered 'In Part' or 'No", please explain your answer.
11	The SOCI Act has increased executive and board focus on critical infrastructure security? Y/N
11(a)	Please explain your answer.
12	How effective is the SOCI Act in addressing current cyber threat environments?
13	How effective is the SOCI Act in addressing current natural hazard and physical threat environments?
14	How effective is the SOCI Act in addressing current supply chain threat environments?

15	How effective is the SOCI Act in addressing current personnel threat environments?
Section 3: Unintended Consequences and Emerging Threats	**Questions**
16	Has the SOCI Act resulted in any unintended impacts or consequences for your organisation (e.g. duplication, delays, burden)?
17	Are there regulatory areas where duplication or overlap occurs (e.g., privacy, APRA CPS 230)?
17(a)	If you answered 'Yes', please explain
18	The SOCI Act has resulted in higher compliance costs than expected? Y/N
18(a)	If you answered 'Yes', please explain
19	The SOCI Act has introduced uncertainty or confusion around allocation of risk and responsibilities? Y/N
19(a)	If you answered 'Yes', please explain
20	How effective is the SOCI Act's framework in supporting continuous improvement and uplift in critical infrastructure security?
21	What are the main improvements you would recommend to ensure the SOCI Act remains fit-for-purpose?
22	What additional guidance, tools or support would assist compliance?

APPENDIX D

MENTIMETER QUESTIONS

Table 7: Mentimeter Questions

Number	Question
1	Is the SOCI Act equipped to deal with emerging threats?
1b	Do current asset classes allow future identification of new classes?
2	Does the SOCI Act support resilience of critical infrastructure?
3	What are the main areas for improvement?
4	Are the obligations in the SOCI Act clear?
5	Suggestions to improve specific obligations
6	Have you experienced issues with definitions?
7	Which definitions cause issues and suggested improvements
8	Are penalties for non-compliance effective/adequate?
9	Anything else?

APPENDIX E

STAKEHOLDER CONSULTATION

Trusted Information Sharing Network	Sector groups

Commonwealth Government	Departments

Peak and Professional Bodies	Organisations

APPENDIX F

LIST OF PUBLIC SUBMISSIONS

The following list includes organisation and individuals who provided a public submission to the review. Several confidential submissions were received that cannot be published below.

Organisation
Personal submissions (4)
Australia Myanmar Institute for Democracy, Human Rights and Peace
The Association of Superannuation Funds of Australia
Water Services Association of Australia
The Business Council of Australia
CI-ISAC Australia
Origin Energy
Vocus
PMT Security Systems
Pentagram Advisory
.au Domain Administration Limited
MPS People Security Risk Management Pty Ltd
Australian Telecommunications Alliance
DroneShield
Global Shield Australia
Australian Banking Association
Transport for NSW
AEMO
CISO Lens
Palo Alto Networks (Australia) PTY LTD
Microsoft
Space Industry Association Of Australia (SIAA)
Good Ancestors Policy
SAP Australia Pty Ltd
Vaesec
Consult Australia
Australian Institute of Company Directors
Australian Small Business and Family Enterprise Ombudsman

APPENDIX G

LIST OF REVIEWED DOCUMENTS AND REFERENCES

Australian Strategic Policy Institute. (2019). *Protecting critical national infrastructure in an era of IT and OT convergence* (R. Shah, Author). Retrieved January 21, 2026, from https://www.aspi.org.au/report/protecting-critical-national-infrastructure-era-it-and-ot-convergence/

Christopher, J. D. (2025). *State of ICS/OT security 2025* (SANS Survey). SANS Institute. Retrieved January 21, 2026, from https://www.sans.org/white-papers/state-ics-ot-security-2025/

Cybersecurity and Infrastructure Security Agency (CISA). (2024, February 23). *Top cyber actions for securing water systems*. Retrieved January 21, 2026, from https://www.cisa.gov/resources-tools/resources/top-cyber-actions-securing-water-systems

Cyber and Infrastructure Security Centre. (2024). *Security of Critical Infrastructure Act 2018 (SOCI)*. Australian Government. https://www.cisc.gov.au/legislation-regulation-and-compliance/soci-act-2018

Newton-Smith, C. (2025). *Supply chain cyberattacks are becoming unmanageable - and UK businesses are paying the price*. TechRadar Pro. Retrieved January 21, 2026, from https://www.techradar.com/pro/supply-chain-cyberattacks-are-becoming-unmanageable-and-uk-businesses-are-paying-the-price

Shah, R. (2019). Assuring the security of our critical infrastructure. *The Strategist*. Australian Strategic Policy Institute. Retrieved January 21, 2026, from https://www.aspistrategist.org.au/assuring-the-security-of-our-critical-infrastructure/

Trend Micro Research. (2025). *Earth Ammit disrupts drone supply chains through coordinated campaigns*. Trend Micro. Retrieved January 21, 2026, from https://www.trendmicro.com/en_us/research/25/e/earth-ammit.html

World Economic Forum. (2025). *Global cybersecurity outlook 2025*. Retrieved January 21, 2026, from https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

World Economic Forum. (2026). *Global cybersecurity outlook 2026*. Retrieved January 21, 2026, from https://www.weforum.org/publications/global-cybersecurity-outlook-2026/

Other literature reviewed (as of January 26th 2026)

Attorney-General's Department. (2022). *Security of Critical Infrastructure (Definitions) Instrument (LIN 22/031) 2022*. Australian Government. https://www.legislation.gov.au/F2023L00006/asmade/2023-01-03/text/original/pdf

Cyber and Infrastructure Security Centre. (2024). *CISC factsheet: SOCI obligations. Australian Government*. https://www.cisc.gov.au/resources-subsite/Documents/cisc-factsheet-soci-obligations.pdf

Cyber Security Agency of Singapore. (2018). *Cybersecurity Act 2018*. Singapore Statutes Online. https://sso.agc.gov.sg/Acts-Supp/9-2018/

Cyber Security Agency of Singapore. (2022). *Critical information infrastructure*. https://isomer-user-content.by.gov.sg/36/2df750a7-a3bc-4d77-a492-d64f0ff4db5a/CCoP---Second-Edition_Revision-One.pdf

Department for Science, Innovation and Technology. (2025). *Cyber Security and Resilience Bill policy statement. UK Government.* https://www.gov.uk/government/collections/cyber-security-and-resilience-bill

Department for Science, Innovation and Technology. (2025). *Cyber Security and Resilience (Network and Information Systems) Bill factsheets*. UK Government. https://www.gov.uk/government/publications/cyber-security-and-resilience-network-and-information-systems-bill-factsheets

Department of Home Affairs. (2021). *Security Legislation Amendment (Critical Infrastructure) Act 2021*. Australian Government. https://www.legislation.gov.au/Details/C2021A00124

Department of Home Affairs. (2022). *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022*. Australian Government. https://www.legislation.gov.au/Details/C2022A00033

Department of Justice Canada. (2024). *Charter Statement: Bill C-26, An Act respecting cyber security. Government of Canada*. https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c26_1.html

European Commission. (2023). *NIS2 Directive: Securing network and information systems*. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

European Commission. (2024). *Critical infrastructure protection & resilience - The CER and NIS2 Directives enter into application*. https://ec.europa.eu/newsroom/cipr/items/859754/

European Cyber Security Organisation. (2025). *NIS2 Directive transposition tracker*. https://ecs-org.eu/activities/nis2-directive-transposition-tracker/

European Parliament and Council. (2022). *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive)*. Official Journal of the European Union, L 333, 80-152. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

European Parliament and Council. (2022). *Directive (EU) 2022/2557 on the resilience of critical entities (CER Directive)*. Official Journal of the European Union, L 333, 164-198. https://eur-lex.europa.eu/eli/dir/2022/2557/ojhttps://eur-lex.europa.eu/eli/dir/2022/2557/oj

Fasken. (2025). *Bill C-8 reboots Canada's cybersecurity legislation for the telecommunications sector and other critical infrastructure*. https://www.fasken.com/en/knowledge/2025/10/bill-c-8

Fasken. (2025). *Prorogations digital impact: Canada's digital bills set to die on the Order Paper*. https://www.fasken.com/en/knowledge/2025/01/prorogations-digital-impacthttps://www.fasken.com/en/knowledge/2025/01/prorogations-digital-impact

House of Commons Library. (2025). *Cyber Security and Resilience (Network and Information Systems) Bill 2024-26*. UK Parliament. https://commonslibrary.parliament.uk/research-briefings/cbp-10442/

Information Commissioner's Office. (n.d.). *The guide to NIS. UK Government*. https://ico.org.uk/for-organisations/the-guide-to-nis/

National Protective Security Authority. (n.d.). *About NPSA: Critical National Infrastructure*. UK Government. https://www.npsa.gov.uk/about-npsa/critical-national-infrastructure

Parliament of Australia. (2018). *Security of Legislation of Critical Infrastructure Act 2018*. https://www.legislation.gov.au/Details/C2018A00029

Parliament of Canada. (2022). Bill C-26: *An Act respecting cyber security, amending the Telecommunications Act*. https://www.parl.ca/legisinfo/en/bill/44-1/c-26

Parliament of Canada. (2025). *Bill C-8: An Act respecting cyber security, amending the Telecommunications Act*. https://www.parl.ca/legisinfo/en/bill/45-1/c-8

Parliament of the United Kingdom. (2025). *Cyber Security and Resilience (Network and Information Systems) Bill 2024-26*. https://bills.parliament.uk/bills/3745

Public Safety Canada. (2024). *Adapting to evolving threats: A summary of Critical 5 approaches to critical infrastructure security and resilience*. Government of Canada. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2024-dptng-vlvng-thrts/index-en.aspx

Public Safety Canada. (2024). *Canada's critical infrastructure*. Government of Canada. https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/cci-iec-en.aspx

Public Safety Canada. (2024). *Q&A: Critical Cyber Systems Protection Act*. Government of Canada. https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20250226-1/07-en.aspx

Public Safety Canada. (2025). *Bill C-8: An Act respecting cyber security*. Parliament of Canada. https://www.parl.ca/legisinfo/en/bill/45-1/c-8

Tunney, C. (2024). *Senators amend error in cybersecurity bill that could have cancelled half of it*. CBC News. https://www.cbc.ca/news/politics/cybersecurity-bill-c26-senate-amend-1.7401358

UK Department for Science, Innovation and Technology. (2023). *The NIS Regulations 2018*. UK Government. https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018

APPENDIX H

MENTIMETER RESULTS FROM TOWN HALL AND TISN MEETINGS

These results are based on the feedback at the large town hall meeting with more than 460 attendees plus smaller TISN meetings.

Table 9: Which sector are you from?

Metric	Details
Total respondents	248
Top sectors	Energy Sector: 57 (largest group) Government / Peak Bodies: 54 Transport: 29 Health Care & Medical: 23 Water & Sewerage: 23
Other sectors	Communications (14), Data Storage (13), Financial Services (12), Higher Education (10), Food & Grocery (6), Space (5), Defence Industry (2)
Insight	Energy and Government dominate feedback, suggesting their views heavily influence overall sentiment.

Table 10: How would you describe the SOCI Act and subordinate legislation?

Metric	Details
Total respondents	244
Top sectors	• complex / complicated / confusing (dominant theme) • toothless (perceived lack of enforcement) • fragmented / overlapping / duplication • risk-based (some positive tone) • good start / evolving (minor positive sentiment).
Other sectors	~70% negative (complexity, ambiguity, duplication) ~20% neutral ~10% positive
Insight	Complexity and lack of clarity are the biggest pain points across sectors.

Table 11: Is the SOCI Act equipped to deal with emerging threats?

Metric	Details
Total respondents	223
Response distribution	Majority: No (dominant response) Partial / Somewhat: Common but still minority Yes: Very few
Reasons cited	• legislation is too slow compared to evolving threats • cyber-heavy focus, neglecting physical and personnel security • lack of hazard-agnostic approach • funding gaps and unclear enforcement.
Insight	Strong perception that SOCI is reactive, not proactive.

Table 12: Main areas for improvement

Metric	Details
Total respondents	192
Top recurring themes	• simplification & clarity: plain English, reduce legal jargon • sector-specific guidance: tailored rules, templates, examples • reduce duplication: align with other Acts (Telco, PSPF, State rules) • physical security standards: not just cyber • clearer definitions: critical worker, asset, protected info

	• funding support: especially for state-owned entities • accountability & enforcement: stronger penalties, audits • integration: with state frameworks and emergency management • international alignment: ISO, NIST.
Insight	Stakeholders want clarity, practicality, and harmonisation with existing frameworks.

Table 13: Are the Obligations clear?

Response	Count
Yes	77
No	118
Unsure	35
Insight	Over half find obligations unclear, reinforcing the need for better guidance.

Table 14: Suggestions for improving obligations

Response	Count
Total responses	174
Common suggestions	• sector-specific obligations and clarity • simplify and standardise requirements • clearer definitions for critical worker, asset, protected info • mandate physical security standards • provide templates and practical examples • remove duplication with other frameworks • introduce tiered obligations based on criticality • improve CIRMP guidance and make it auditable • stronger penalties for boards and directors • better integration with state rules and emergency arrangements.
Insight	Practicality and enforceability are key priorities.

Table 15: Issues with Definitions

Response	Count
Yes	177
No	26
Unsure	14
Insight	Definitions are a major pain point.

Table 16: Common Definition issues

Category	Issues identified
Key problems	Ambiguity and inconsistency Critical worker definition too broad or unclear Protected information hard to interpret Asset vs infrastructure confusion IT vs OT unclear "Relevant impact" and "material risk" vague Responsible entity vs service provider unclear

	Sector-specific nuances missing
Insight	Definitions need sector-specific clarity and harmonisation.

Table 17: Are penalties effective?

Metric	Details
Response	Overwhelming majority: No
Common comments	• what penalties? • toothless • not enforced • boards don't care • easier to pay fine than comply.
Insight	Lack of enforcement undermines compliance and board engagement.

Table 18: Additional comments – key themes

Category	Themes
Key feedback	• good start but needs evolution • too complex, legalistic, and duplicative • needs clarity, sector-specific rules, and practical guidance • funding gaps are a major barrier • penalties need to be stronger and enforced • better integration with other legislation and state frameworks • focus on real security uplift, not just compliance • more engagement and education for boards and executives • physical security and supply chain risks need more attention • international alignment and lessons from other countries suggested.
Insight	Stakeholders want SOCI to move from compliance-driven to outcome-driven.

Data collected via Mentimeter during town hall (460+ attendees) and TISN meetings

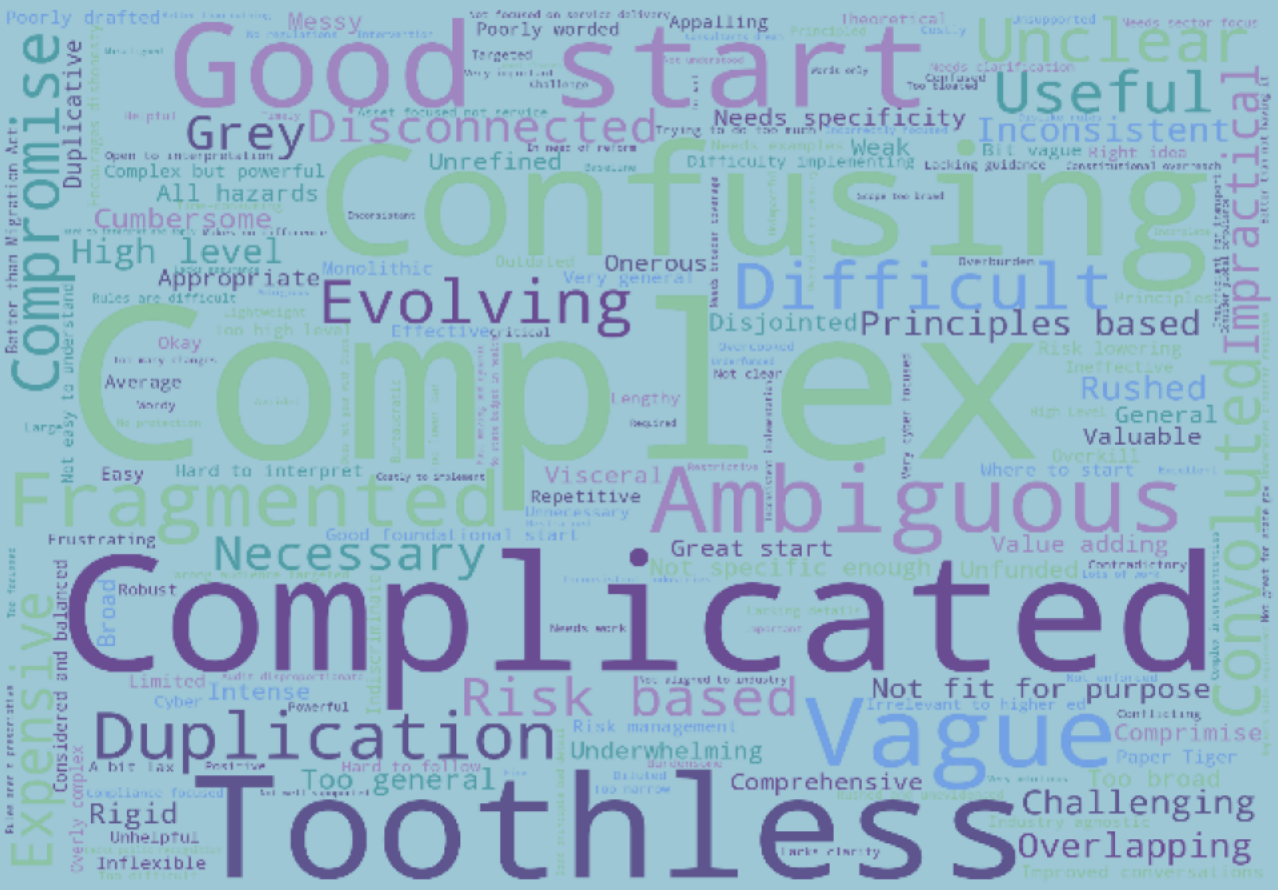


Figure 4: Word cloud from the responses to '*From your experiences interacting with SOCI legislation, in one or two words how would you describe the SOCI Act and subordinate legislation?'*

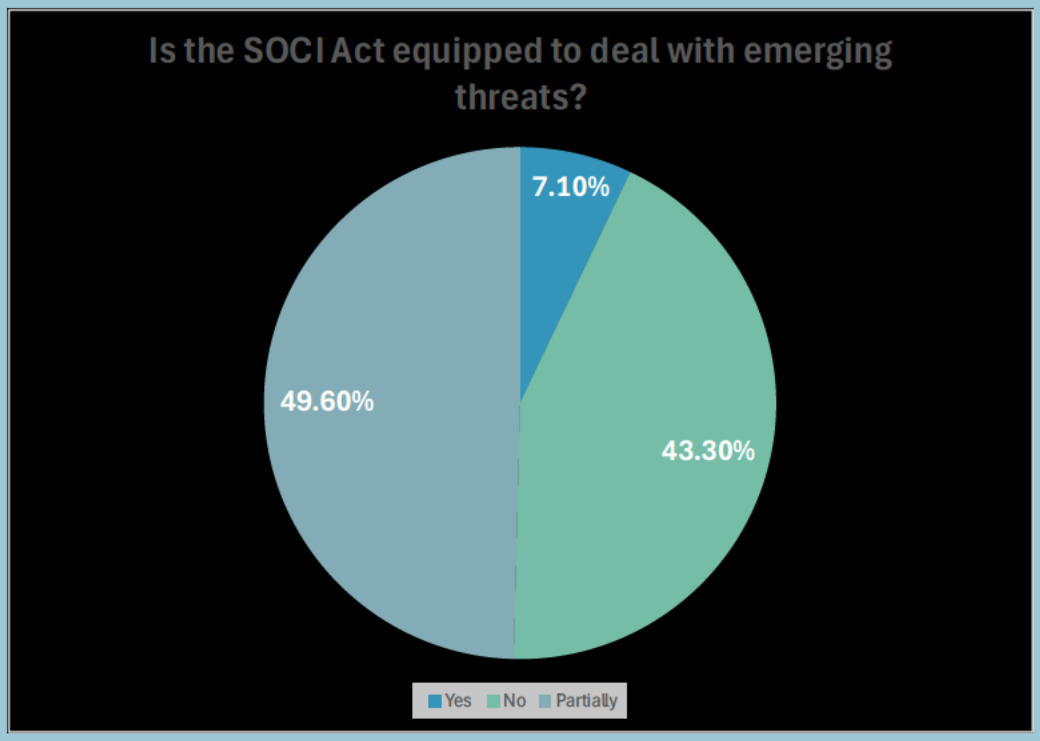
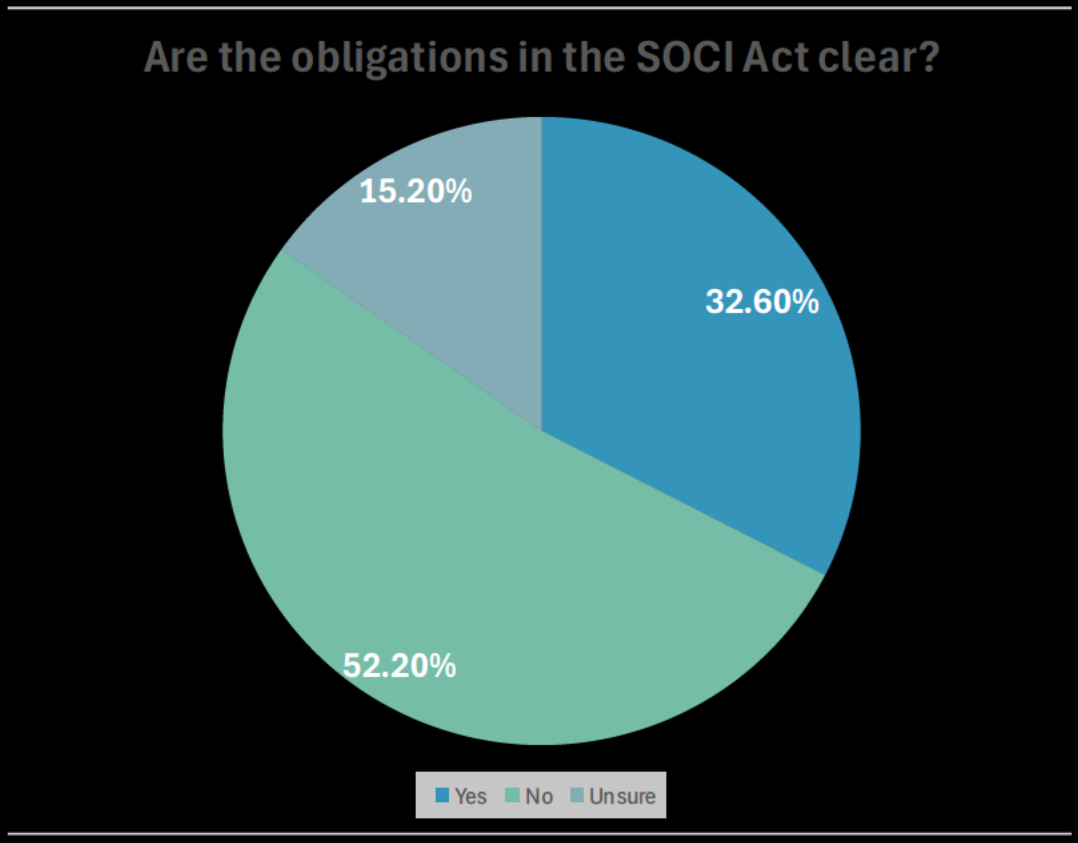


Figure 5: Pie chart from the responses to *'Is the SOCI Act equipped to deal with emerging threats?'*


Flexibility through vagueness
Encourages CIRMPs
Rigid and siloed
Principles-based approach
Compliance burden
Cost pass-through
Government-industry collaboration
AI and advanced tech gaps
State vs. federal clarity
Dynamic threat environment
Insufficient funding
Limited sector coverage
Hazard-agnostic approach
Poor alignment
Overemphasis on cyber
Point-in-time nature
Lagging behind threats
Baseline framework
Supply chain vulnerabilities


Are the obligations in the SOCI Act clear?
15.20%
32.60%
52.20%
Yes
No
Unsure

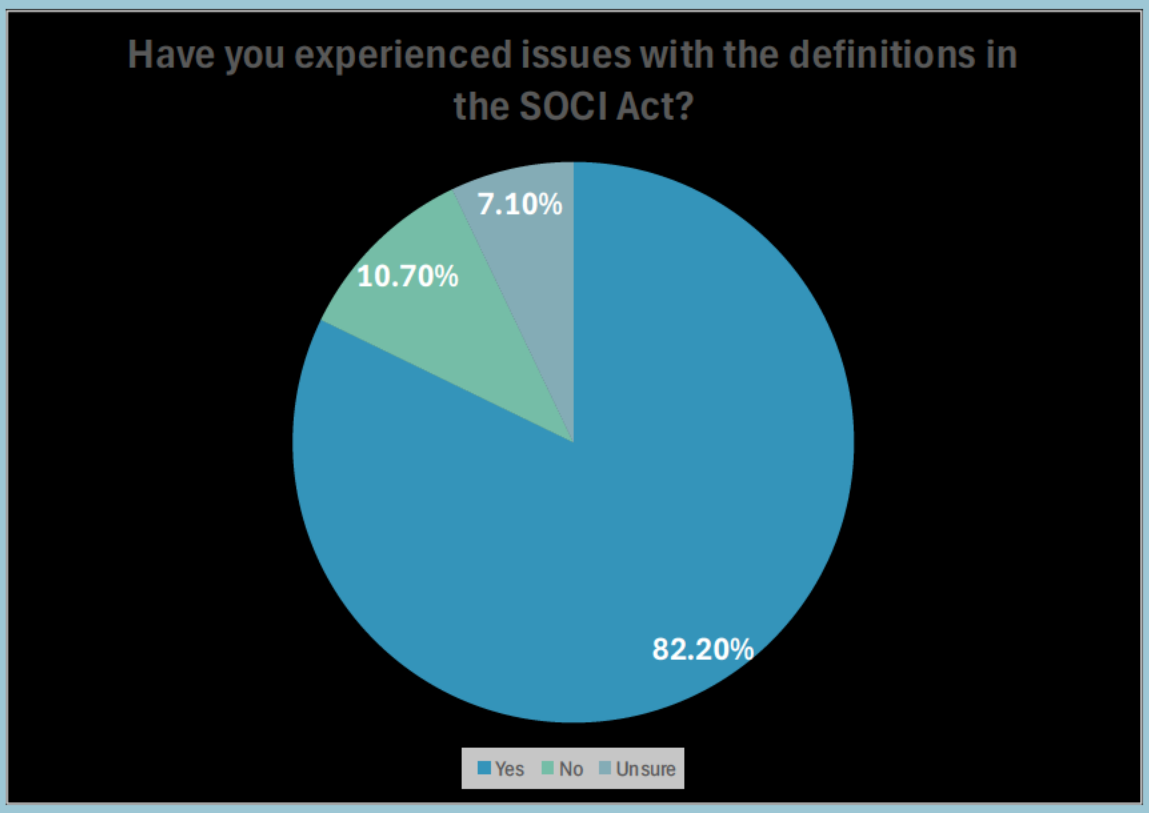


Figure 8: Pie chart from responses to *'Have you experienced issues with the definitions in the SOCI Act (including subordinate legislation)?'*

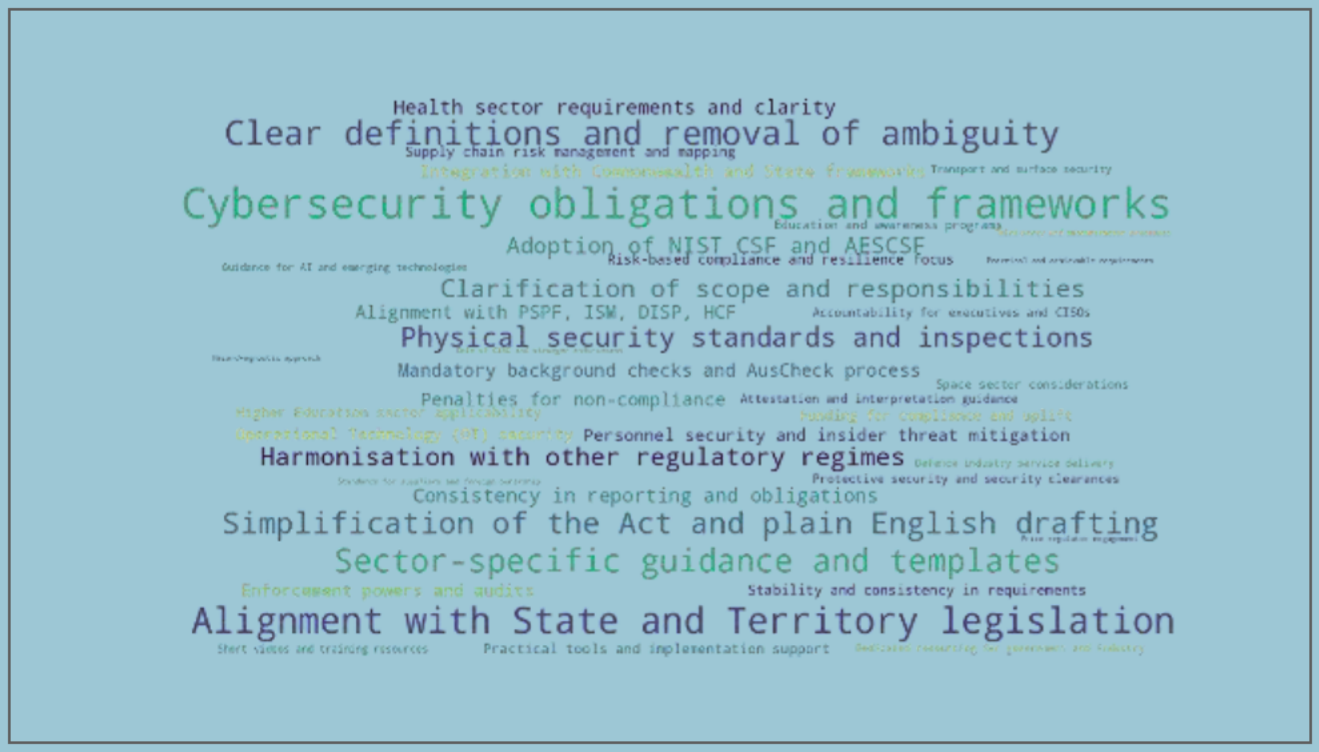


Figure 9: Word cloud from the responses to *'What are the main areas for improvement of the SOCI Act and subordinate legislation?'*

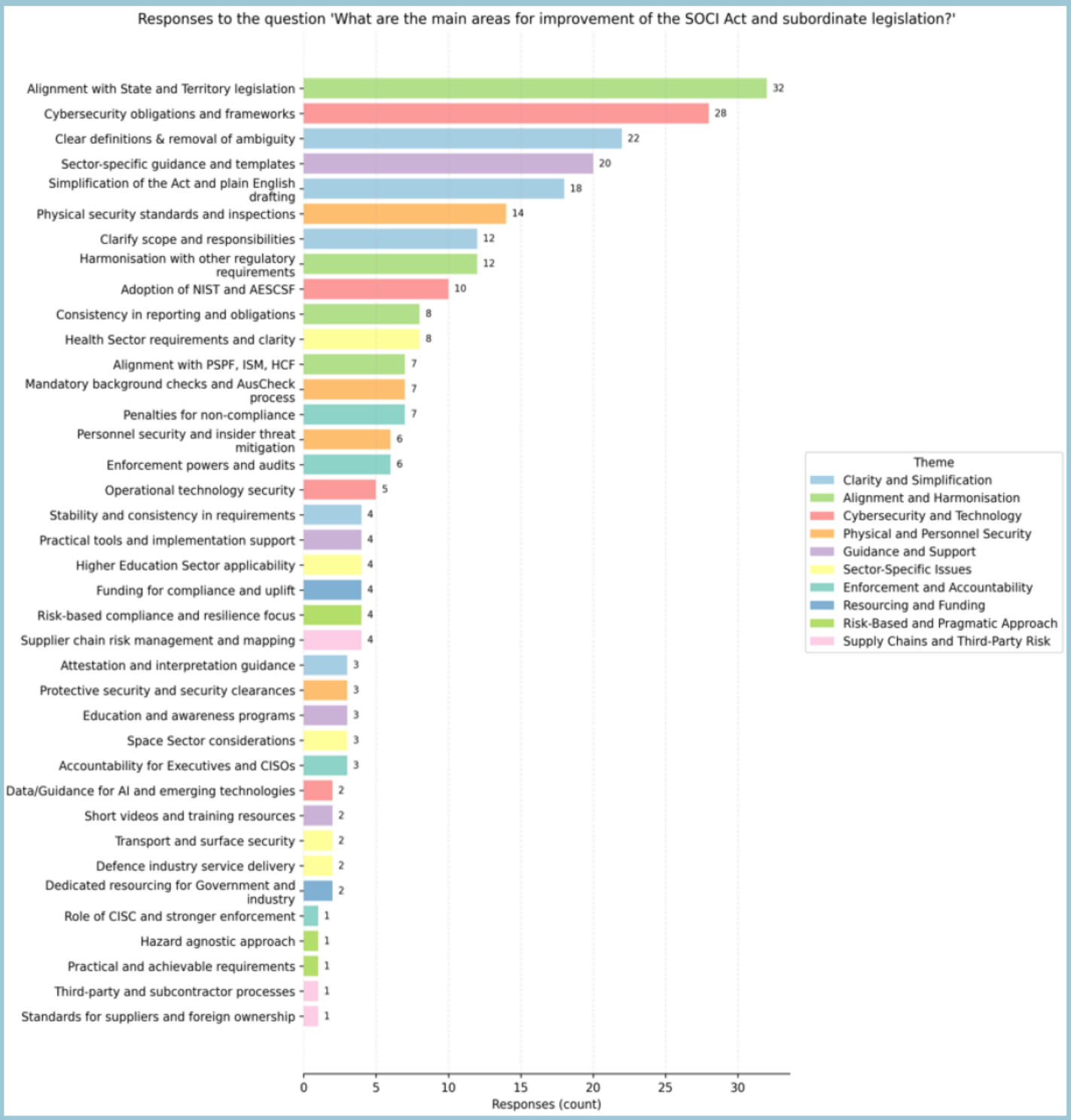


Figure 10: Bar chart from the responses to *'What are the main areas for improvement of the SOCI Act and subordinate legislation?'*

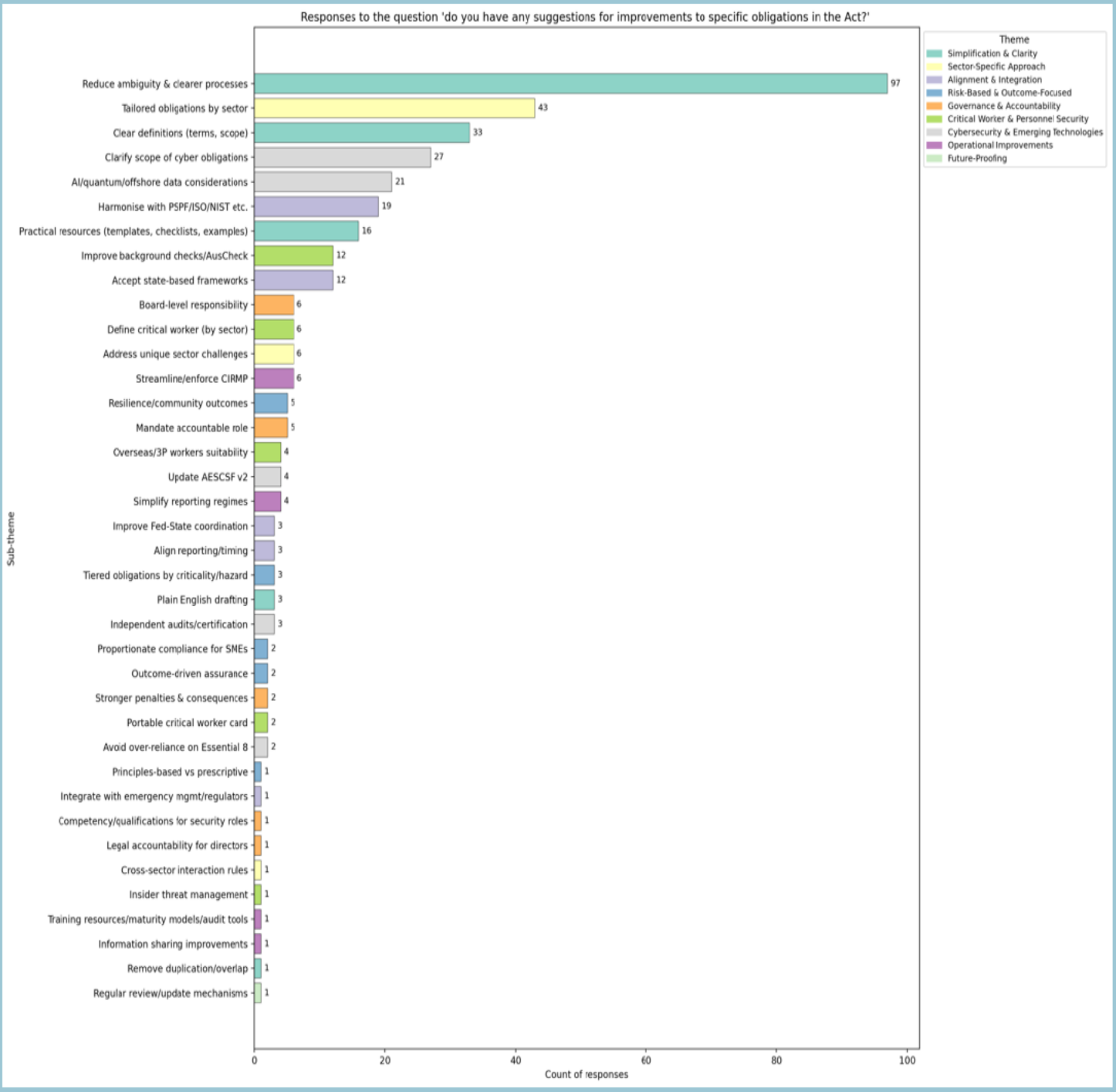


Figure 11: Bar chart from the responses to '*Do you have any suggestions for improvements to specific obligations in the Act?*'

APPENDIX I

CONSOLIDATION OF SURVEY RESULTS

Introduction

This report shows the consolidation of survey results for the TISN Townhall, REAG, SCEAG, TISN Government and TISN Leadership cohorts. A total of **89** people responded. However, some questions were not mandatory for participants to answer, and therefore the responses are not indicative of the full cohort of respondents. Not all questions would apply to every respondent.

Pre-survey - Respondent Information

Pre-survey - Which sector does your organisation operate in?

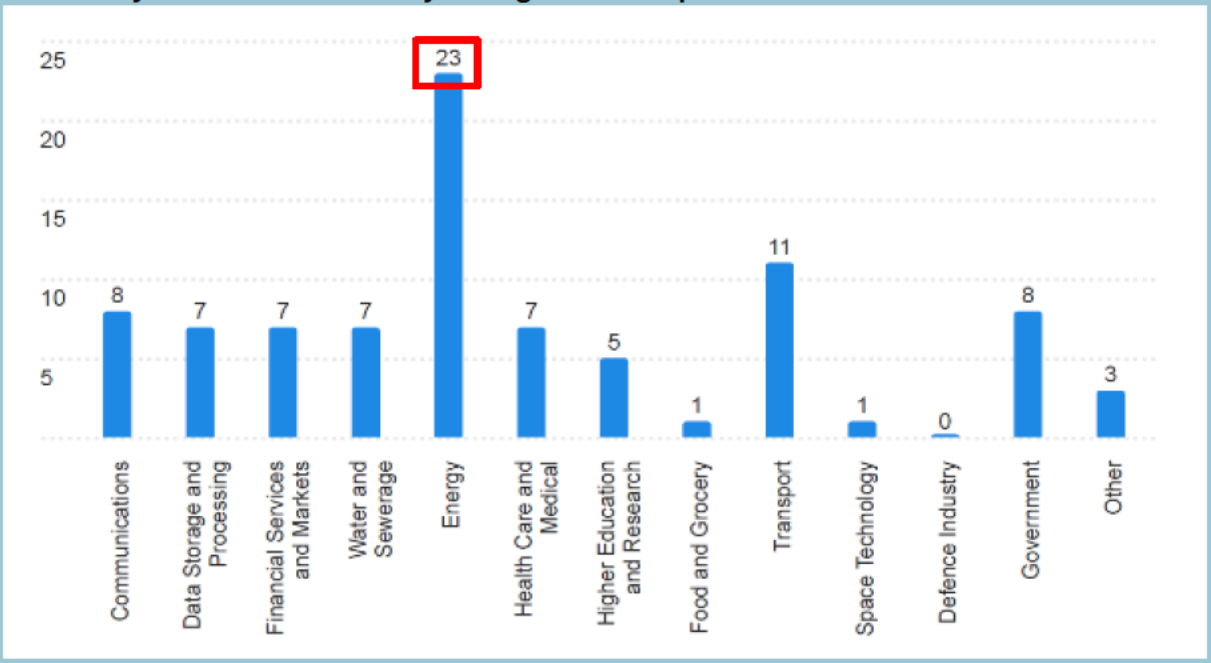


Figure 12: Bar chart from the responses to pre-survey question '*Which sector does your organisation operate in?*'

Please note:

- 'other' refers to peak bodies, consultants, academics etc.
- the number of responses appears above each bar on the graph (see highlighted in red).

Pre-survey - If you selected 'other', please specify:

Three responses were received for this question:

- Port Authority
- we work in both Government and Defence Industry
- government regulator.

Pre-survey - What is the size of your organisation?

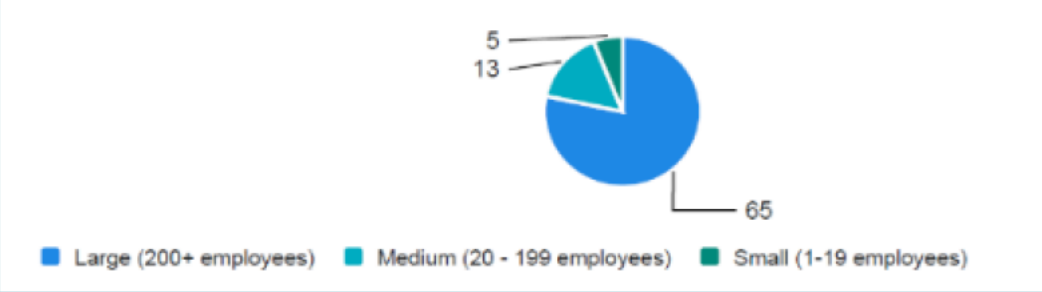


Figure 13: Pie chart from the responses to '*What is the size of your organisation*?'

Pre-survey - What is your job title?

Table 19: Responses to 'What is your job title?'

Response
Associate OT Engineer
General Manager
APAC Business Resilience Manager
Public Servant
Commercial Operations Manager
Policy and Government Relations
Category Manager – Directs, Procurement
Government and Regulatory Affairs
General Manager - Regulatory and REAG member
Global Security
Airport Manager
Director of Cybersecurity
Security and Emergency Response Supervisor
Group Workplace, Health, Safety, Environment and Social (WHSES) Manager
Sales Director
Security Risk Manager
Cyber Security Lead
Security Compliance Specialist
OT Cybersecurity Manager
General Manager – Regulatory Affairs

Section 1: Achievement of Intended Objectives

Q1 - To what extent has the SOCI Act improved the security and resilience of your organisation's critical infrastructure?

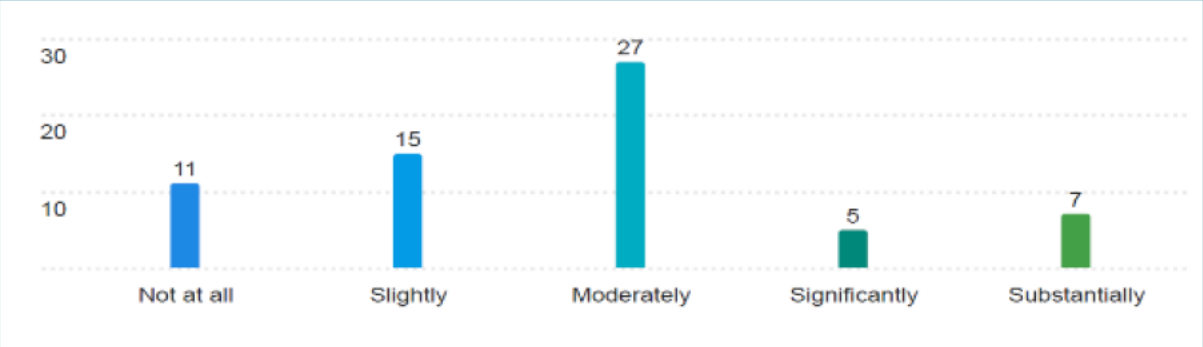


Figure 14: Bar chart for the responses to '*To what extent has the SOCI Act improved the security and resilience of your organisation's critical infrastructure?*

Q2 - In your view, what elements of the SOCI Act have been the most effective in meeting its intended objectives?

A summary of the responses provided is below:

- improved awareness: organisations are more aware of cyber and physical threats and better at identifying critical areas
- clearer framework: moving Part 14 of the Telecommunications Act into SOCI strengthened clarity and robustness
- risk management uplift: CIRMP requirements and multi-hazard approach drove collaboration across functions and improved supply chain and personnel security
- executive engagement: reporting obligations and penalties increased board-level focus; some suggest higher fines for stronger compliance
- improved industry and government collaboration: some said that SOCI clarified accountabilities and boosted information sharing across industry and government.

Q3 - In your view, which aspects of the SOCI Act have been the most challenging to implement for your organisation?

A summary of the responses provided is below:

- clarity and interpretation issues: some respondents found SOCI obligations vague, with broad definitions (e.g., "significant impact") and unclear registration processes
- duplication and overlap: significant crossover with other frameworks (APRA CPS 230/234, Cyber Security Act, Aviation Transport Security Act, DISP, HCF), creating administrative burden
- integration problems: requirement for separate CIRMP documentation conflicts with existing Enterprise Risk Management programs
- supplier and protected information: difficulty notifying suppliers and sharing details due to confidentiality and regulatory constraints.
- personnel security and timeliness: background checks and compliance timelines were challenging.
- complexity and cost: rapid regulatory changes within fixed funding cycles and ongoing uplift requirements strain budgets.
- sector-specific issues: telco-specific concerns (e.g., E8 ML1 TSRMP requirement) and aviation asset definition inconsistencies.
- mixed experiences: some organisations report minimal challenges, citing structured approaches and mature governance.

Q4 - Has your organisation experienced any operational or administrative challenges complying with the SOCI Act?

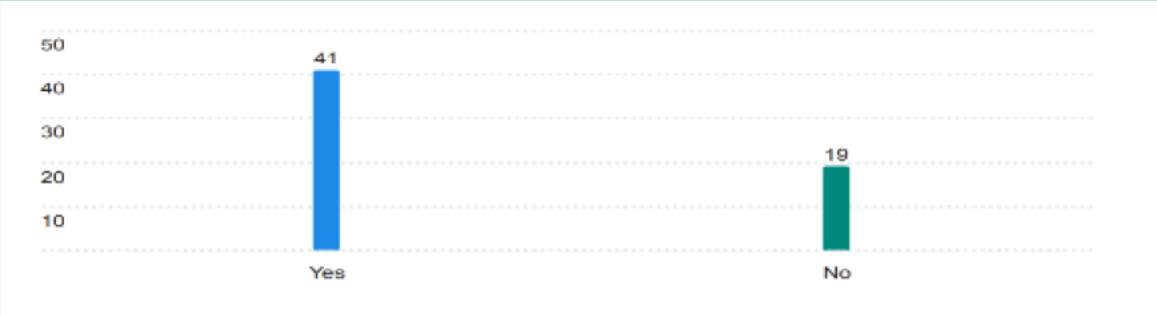


Figure 15: Bar chart for the responses to '*Has your organisation experienced any operational or administrative challenges complying with the SOCI Act?'*

Q4(a) - If you answered 'Yes', please briefly describe:

A summary of the responses provided is below:

- vague requirements and interpretation issues: unclear definitions (e.g., critical assets, risk levels, "significant impact"), vague personnel security vetting guidance, and inconsistent regulator responses make compliance difficult
- integration and change fatigue: frequent amendments and the need for separate CIRMP documentation hinder embedding SOCI into existing Enterprise Risk Management programs
- administrative burden: heavy reporting requirements, complex online formats, and overly detailed CIRMP expectations increase workload without adding operational value
- resource and budget constraints: compliance is costly and labour-intensive, especially for large organisations with competing priorities; recruitment of cyber security personnel is challenging.
- supplier and third-party issues: contract negotiations and protected information sharing create delays and uncertainty.
- duplication and misalignment: overlap with other frameworks (APRA CPS 230/234, DISP, Aviation Transport Security Act) and inconsistent thresholds for reporting add complexity.
- sector-specific and structural challenges: SOCI hazards don't align well with organisational structures; definitions for IT/OT ownership and aviation assets remain problematic.
- operational strain: background checks for critical workers, lack of templates, and unclear risk prioritisation slow implementation.
- mixed engagement: some organisations question whether compliance efforts match actual security outcomes, citing "document warfare" rather than strategic uplift.

Section 2: Functioning of the Act in Practice

Q5 - Does subsection 12F(3) of the SOCI Act clearly explain the requirement to notify data storage or processing providers?

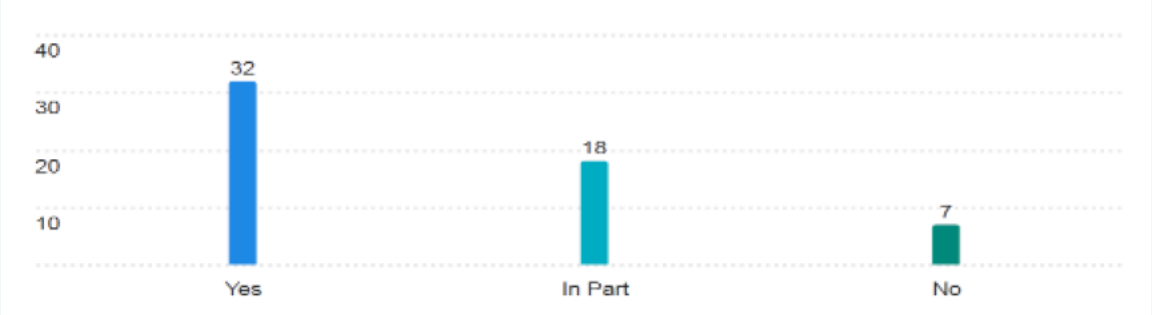


Figure 16: Bar chart for the responses to '*Does subsection 12F(3) of the SOCI Act clearly explain the requirement to notify data storage or processing providers?'*

Q5(a) - If you answered 'In Part' Or 'No', please explain your answer.

A summary of the responses provided is below:

- ambiguity in obligations: unclear boundaries between critical infrastructure assets and suppliers; confusion around what constitutes a third-party data holder and their responsibilities
- notification complexity: difficulty ensuring suppliers understand their obligations; limited ability to influence external parties like major cloud providers (AWS, Azure, Google)
- protected information issues: uncertainty around definitions (e.g., patient data in healthcare) and risks when sharing sensitive information with third parties
- administrative burden: multiple, inconsistent reporting requirements and lack of clear guidance on records to prove notifications were received and understood
- broad and confusing definitions: terms like "business critical data" and supporting systems (e.g., Active Directory, file services) are poorly defined, creating interpretation challenges
- limited practical value: some respondents feel notifications add little security value when providers already comply with other standards
- sector-specific concerns: health and utilities flagged unique challenges in applying SOCI obligations to their contexts.

Q6 - Asset register requirements are clear and practical to implement.

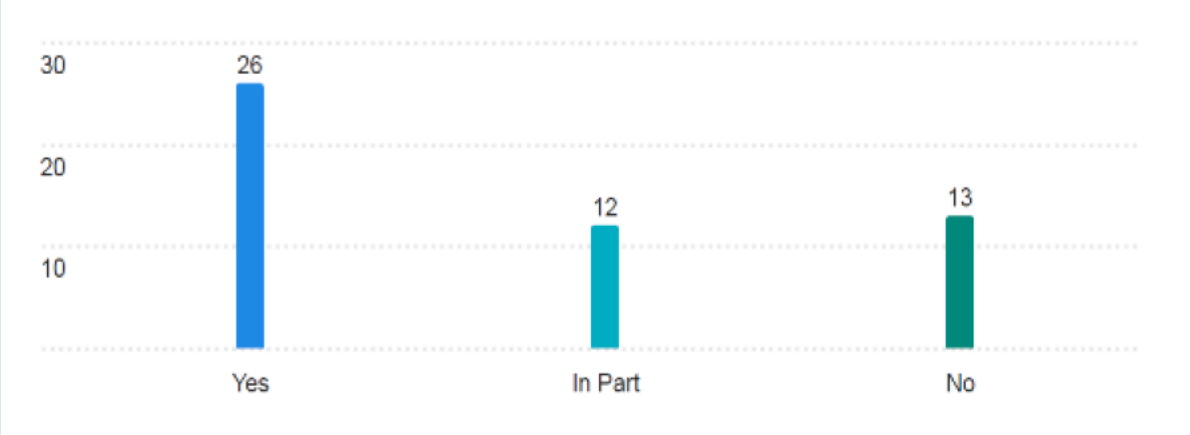


Figure 17: Bar chart for the responses to '*Asset register requirements are clear and practical to implement*'.

Q6(a) - If you answered 'In Part' Or 'No', please explain your answer.

A summary of the responses provided is below:

- ambiguity in definitions and scope: unclear definitions of "critical component," "asset," and thresholds (e.g., 100,000 connections) lead to inconsistent interpretations and reporting
- granularity and practicality issues: requirements to register every component (e.g. pump stations, towers) are seen as overly granular and add little value for holistic risk management
- administrative burden: asset registration and ongoing updates are resource-intensive, especially for organisations with large, complex asset portfolios or multiple CI assets
- sector variability: implementation differs significantly across sectors (Energy, Water, Communications), creating inconsistency and complexity
- integration challenges: organisations must adapt or build internal registers to align with SOCI reporting, causing duplication and inefficiency
- system and process limitations: lack of downloadable forms, unclear reporting processes, and concerns about confidentiality of registration systems hinder compliance
- cross-functional awareness: difficulty coordinating across business units and subsidiaries to ensure accurate reporting
- limited guidance and support: organisations report unclear requirements, slow regulator responses, and reliance on self-interpretation, increasing risk of non-compliance.

Q7- Critical Infrastructure Risk Management Program requirements are clear and practical to implement.

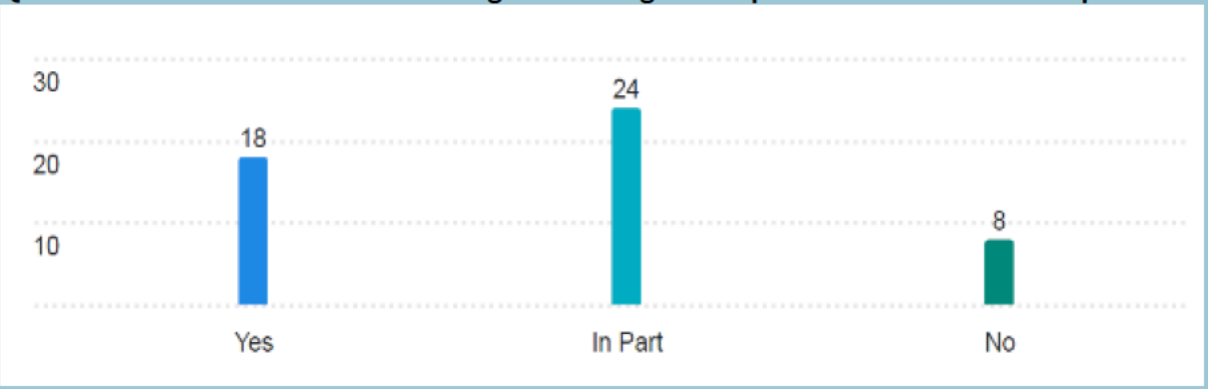


Figure 18: Bar chart for the responses to *'Critical Infrastructure Risk Management Program requirements are clear and practical to implement'*.

Q7(a) - If you answered 'In Part' Or 'No', please explain your answer.

A summary of the responses provided is below:

- ambiguity in CIRMP requirements: definitions and expectations are unclear, making it hard to interpret obligations and integrate CIRMP into existing risk frameworks
- integration and administrative burden: CIRMP adds another layer of documentation, creating complexity and heavier admin rather than streamlined risk management
- conflicting guidance and change fatigue: frequent amendments and inconsistent advice from CISC hinder embedding and create uncertainty
- cyber framework misalignment: existing frameworks (e.g., Essential 8, AESCSF, C2M2) don't fully address all hazard vectors, making compliance fragmented and audits subjective.
- practicality issues: CIRMP obligations are difficult to implement within timeframes, especially for large organisations, multi-sector entities, and critical worker checks
- resource constraints: developing and maintaining CIRMPs requires dedicated staff and budget, which is challenging for organisations with competing priorities
- lack of risk clarity: no defined risk appetite or consistent baseline across sectors; unclear what resilience levels are expected
- documentation vs substance: focus on paperwork rather than intelligence-led, risk-informed practices risks creating systemic vulnerabilities.

Q8 - Telecommunications Security and Risk Management Program requirements are clear and practical to implement.

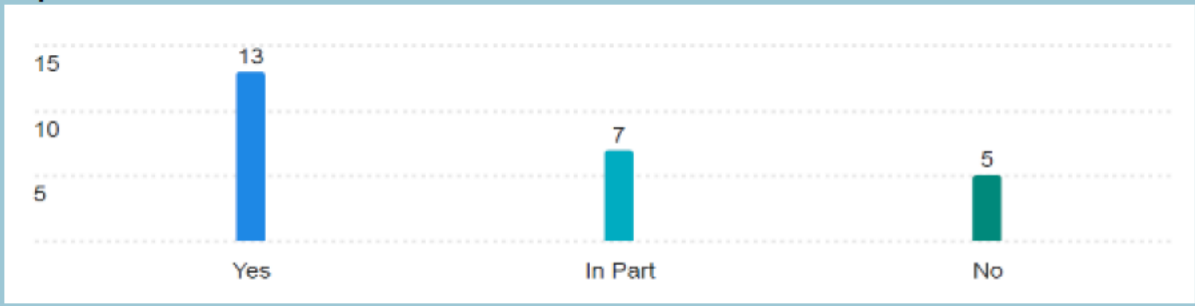


Figure 19: Bar chart for the responses to *'Telecommunications Security and Risk Management Program requirements are clear and practical to implement'*.

Q8(a) – If you answered 'In Part' Or 'No', please explain your answer.

A summary of the responses provided is below:

- ambiguity in requirements: unclear guidance on applying E8 ML1 to telcos and how TSRMP interacts with other telco-specific outage legislation
- duplication and lack of alignment: entities required to produce both CIRMP and TSRMP with no formal guidance on reducing duplicated effort
- poor guidance and no templates: lack of training, templates, and clarity on which risks to prioritise (cybersecurity, supply chain, etc.), especially for smaller ISPs
- limited practical value: TSRMP seen as a "box-checking exercise" with unclear purpose and minimal uplift in actual security outcomes
- resource burden: maintaining TSRMP requires dedicated compliance staff and integration with existing frameworks, creating cost and complexity
- sector-specific complexity: telecommunications networks are highly interconnected, making risk management more challenging than in single-asset sectors
- supply chain dependencies: heavy reliance on overseas vendors introduces risks that are difficult to mitigate
- system gaps: lack of clear redundancies and gaps in coverage (e.g., content delivery networks not included).

Q9 – Mandatory cyber incident reporting thresholds are reasonable and achievable.

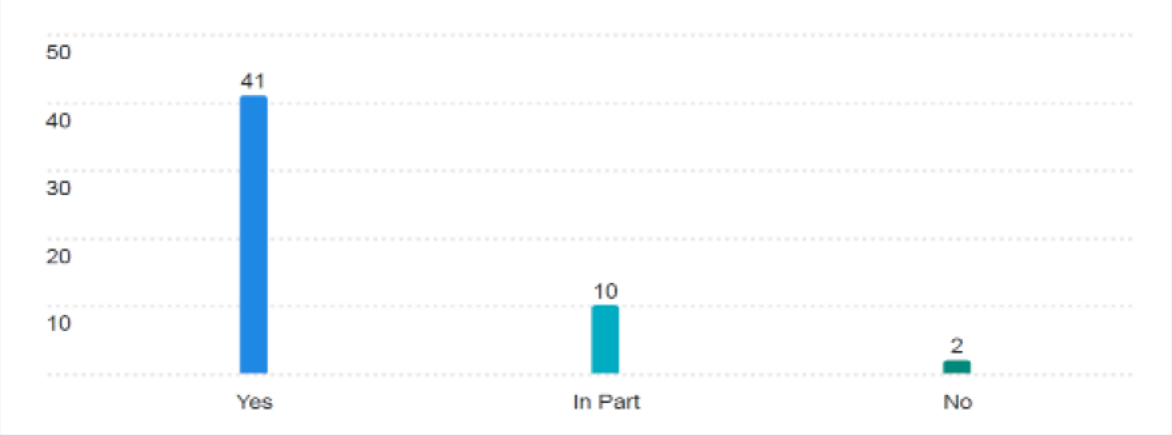


Figure 20: Bar chart for the responses to *'Mandatory cyber incident reporting thresholds are reasonable and achievable'*.

Q9(a) - If you answered 'In Part' Or 'No', please explain your answer.

A summary of the responses provided is below:

- ambiguity in definitions and thresholds: unclear terms like "becoming aware," "serious incident," and "relevant impact" create confusion and require burdensome legal interpretation.
- complexity of assessment: determining whether an incident meets critical or relevant impact criteria is difficult and often requires rapid technical and operational analysis under time pressure
- tight reporting timeframes: the 12-hour window for critical incidents and 72-hour window for others are challenging, especially for organisations with distributed systems or limited response capability
- overlap with other obligations: multiple and inconsistent reporting requirements across SOCI, Privacy Act, APRA CPS 234, and sector-specific standards add complexity
- coordination challenges: involvement of third-party vendors and supply chain partners introduces delays and accountability issues
- resource burden: smaller entities struggle with compliance due to lack of automation and dedicated staff; manual reporting is costly and time-consuming

- data sensitivity and confidentiality: sharing sensitive operational and security information with government agencies raises confidentiality and reputational concerns
- sector variability: different operational realities across sectors (telecom, healthcare, energy) make uniform compliance difficult.

Q10 - The Enhanced Cyber Security Obligations (ESCO), if applicable to your organisation, are proportionate and practicable.

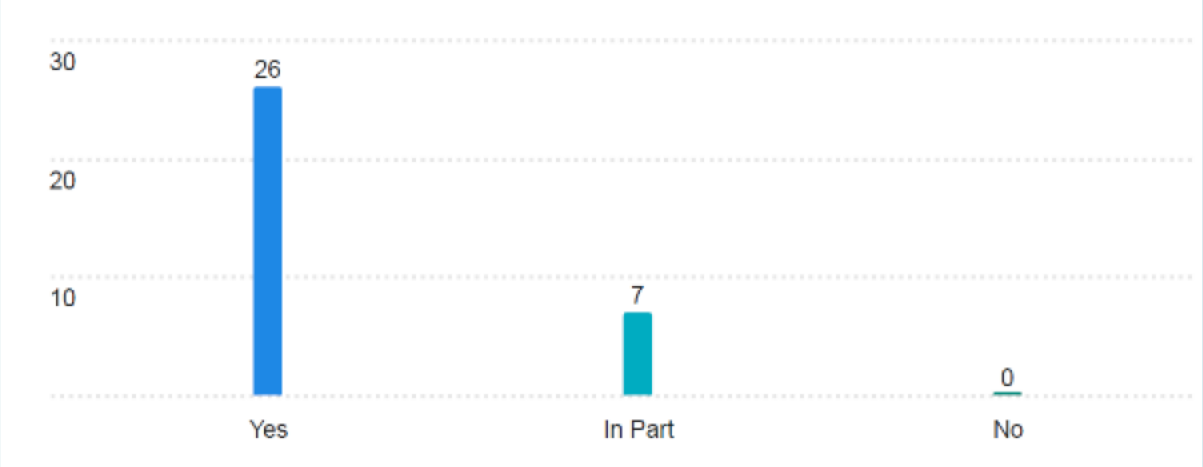


Figure 21: Bar chart for the responses to *"The Enhanced Cyber Security Obligations (ESCO), if applicable to your organisation, are proportionate and practicable'.*

Q10 (a) - If you answered 'In Part' Or 'No", please explain your answer.

A summary of the responses provided is below:

- conflicting cyber maturity obligations: different sectors impose varying maturity requirements, creating complexity for organisations operating across multiple sectors with shared IT/OT/Telco components.
- resource burden: ESCO obligations require advanced cyber capabilities, continuous monitoring, and regular testing—demanding significant investment in people, processes, and technology.
- sector variability: telecommunications, energy, and defence-linked organisations face different levels of complexity, making uniform implementation difficult
- integration and duplication: ESCO requirements must align with existing frameworks (ISO/IEC 27001, NIST CSF, APRA CPS 234), creating overlap and administrative overhead
- information sharing concerns: obligations to provide system details to government raise confidentiality and operational disruption risks
- specialist skills gap: smaller or less mature organisations struggle to meet obligations without external support
- framework misalignment: rules interchange frameworks (Essential 8, AESCSF) with standards, creating vague measures of success and unclear priorities for OT security.
- practicality issues: significant effort required for process design, training, exercises, and testing adds operational strain.

Q11 - The SOCI Act has increased executive and board focus on critical infrastructure security.

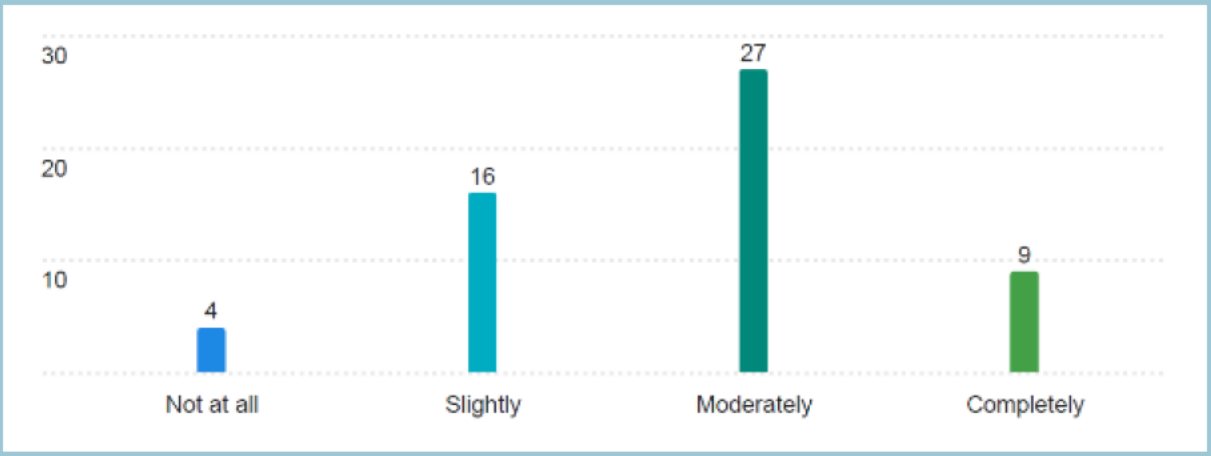


Figure 22: Bar chart for the responses to '*The SOCI Act has increased executive and board focus on critical infrastructure security'*.

Q11(a) – Please explain your answer

A summary of the responses provided is below:

- moderate increase in board engagement: SOCI has prompted more executive and board-level discussions, though some boards only engage annually for compliance rather than ongoing security improvement
- accountability and responsibility challenges: understanding roles remains an issue for some organisations
- spotlight on Risk Management: SOCI has supported comprehensive reviews of hazard vectors and forward planning, often integrated with existing frameworks like APRA CPS 230/234
- mixed depth of engagement: while some boards treat SOCI compliance seriously and link it to funding for improvements, others focus on compliance "tick-box" rather than actual security uplift
- sector variability: universities and entities without critical assets report minimal direct board involvement, relying on compliance registers and attestations
- positive outcomes: increased visibility of cyber and personnel security risks at executive level; some organisations have established SOCI working groups and regular reporting to boards.

Q12 - How effective is the SOCI Act in addressing current cyber threat environments?

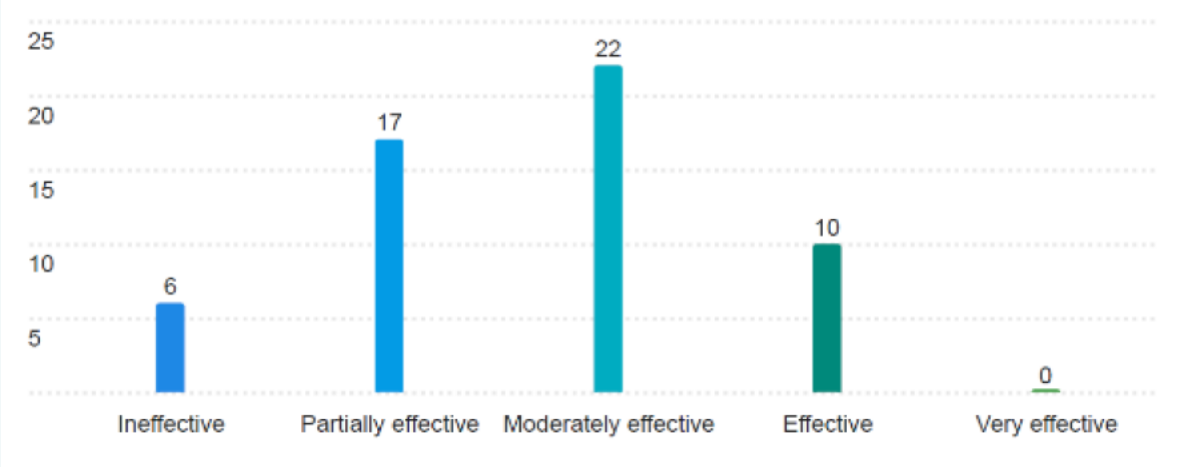


Figure 23: Bar chart for the responses to '*How effective is the SOCI Act in addressing current cyber threat environments?'*

Q13 - How effective is the SOCI Act in addressing current natural hazard and physical threat environments?

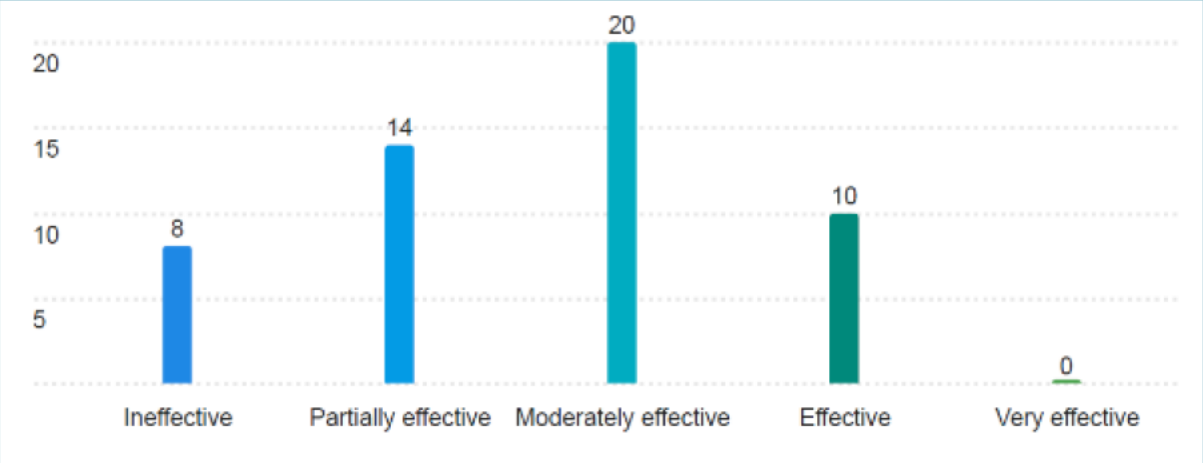


Figure 24: Bar chart for the responses to '*How effective is the SOCI Act in addressing current natural hazard and physical threat environments?*'

Q14 - How effective is the SOCI Act in addressing current supply chain threat environments?

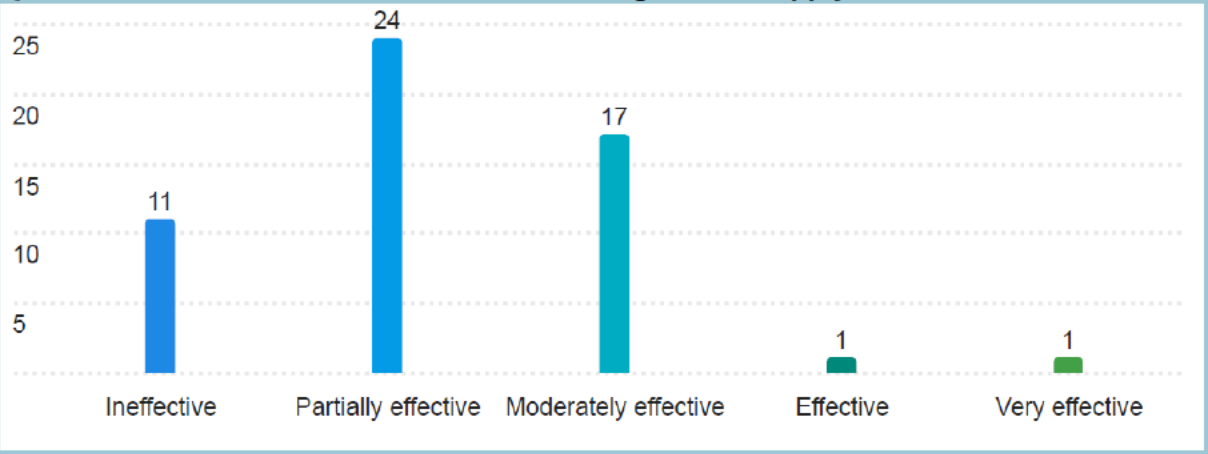


Figure 25: Bar chart for the responses to *'How effective is the SOCI Act in addressing current supply chain threat environments?'*

Q15 - How effective is the SOCI Act in addressing current personnel threat environments?

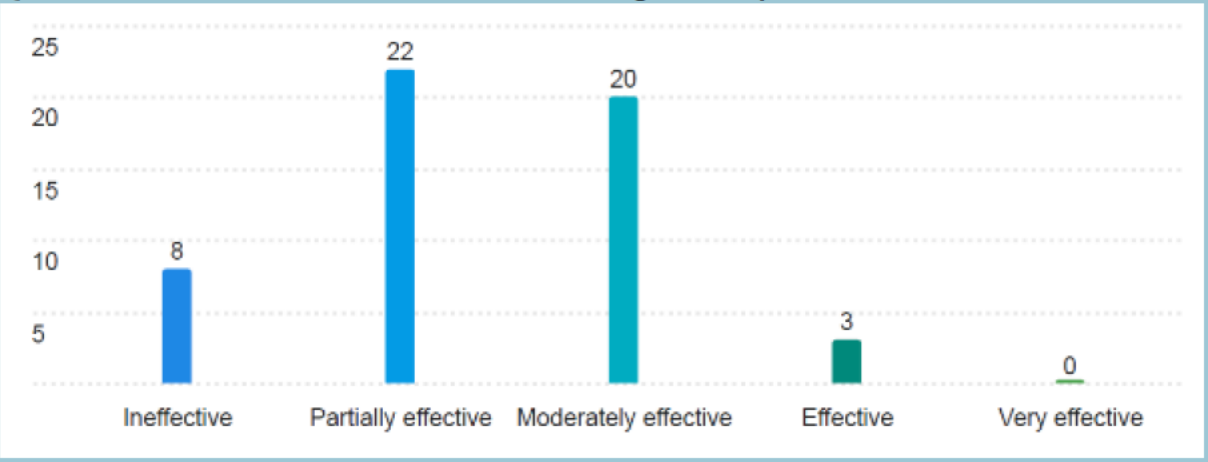


Figure 26: Bar chart for the responses to *'How effective is the SOCI Act in addressing current personnel threat environments?'*

Section 3: Unintended Consequences and Emerging Threats

Q16 - Has the SOCI Act resulted in any unintended impacts or consequences for your organisation (e.g. duplication, delays, burden)?

Figure 27: Bar chart for the responses to '*Has the SOCI Act resulted in any unintended impacts or consequences for your organisation (e.g. duplication, delays, burden)?'*

Q16(a) - Please provide any details regarding Question 16 here:

A summary of the responses provided is below:

- duplication and overlap: SOCI obligations duplicate existing frameworks (e.g., HCF, APRA CPS 234, ISO 27001), creating additional administrative burden and inefficiencies
- integration complexity: multiple functional teams impacted; lack of clarity around terminology and application makes embedding SOCI into existing programs difficult
- constant amendments: frequent changes to obligations create workload strain and hinder development of clear maturity programs
- resource and cost burden: significant investment required for compliance—training, administration, and reporting—especially for large organisations with multiple assets across sectors
- financial constraints: government entities and regulated businesses face challenges funding cyber and resilience measures within fixed budgets
- operational disruption: background checks and clearance processes cause delays and strain on limited security resources
- State vs Commonwealth misalignment: conflicting standards between federal and state requirements create complexity for governance and reporting
- limited practical value: compliance often perceived as adding cost and paperwork without delivering additional security outcomes.

Q17 - Are there regulatory areas where duplication or overlap occurs (e.g. Privacy, APRA CPS 230)?

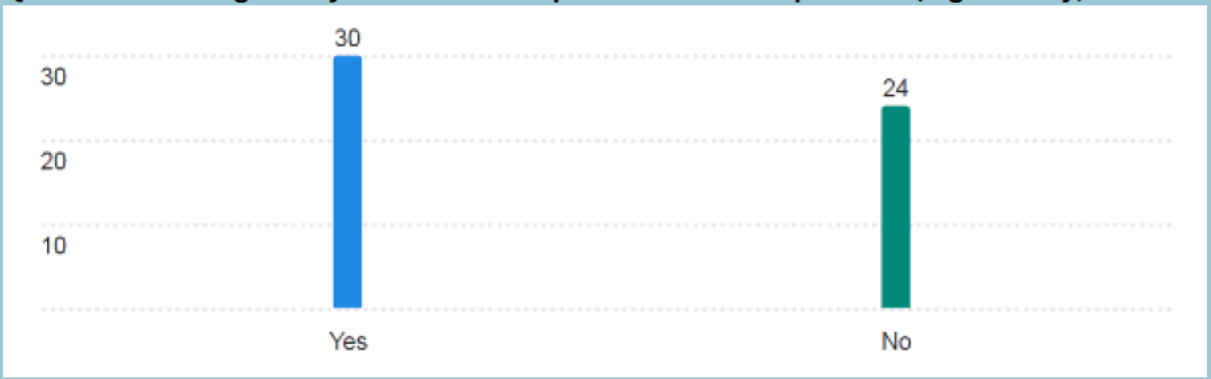


Figure 28: Bar chart for the responses to '*Are there regulatory areas where duplication or overlap occurs (e.g. privacy, APRA CPS 230)?'*

Q17(a) - Please provide any details regarding Question 17 here:

A summary of the responses provided is below:

- significant overlap with other frameworks: SOCI obligations duplicate or intersect with multiple regulatory and security frameworks, including:
    1. APRA CPS 230 & CPS 234 (operational risk and information security)
    2. Privacy Act (data breach reporting and personal information protection)
    3. DISP & PSPF (personnel vetting and protective security)
    4. ISO/NIST standards (cyber and supply chain security)
    5. Sector-specific regulations (Telco legislation, healthcare privacy laws, state-based PSPF)
- duplication of effort: organisations must produce multiple plans (e.g., CIRMP & TSRMP) and attest to overlapping standards, creating administrative burden
- inconsistent definitions and scope: broad definitions like "business critical data" capture personal information beyond SOCI's intent, causing confusion and overlap with Privacy Act obligations
- State vs Commonwealth misalignment: lack of a national approach and conflicting state-level requirements lead to complexity and over-reporting
- supply chain complexity: multiple cyber standards mean vendors must comply with different frameworks for different clients, increasing cost and effort.

Q18 - The SOCI Act has resulted in higher compliance costs than expected

Figure 29: Bar chart for the responses to '*The SOCI Act has resulted in higher compliance costs than expected*'.

Q18(a) - If you answered 'Yes', please explain

A summary of the responses provided is below:

- significant compliance cost burden: organisations report higher-than-expected costs due to expanded reporting requirements, additional security controls, and technology investments
- resource strain: large organisations require extra FTEs and coordination functions to manage SOCI obligations; smaller ISPs face disproportionate cost and training burdens
- administrative overhead: increased documentation, background checks, and maintenance of systems/processes add complexity without corresponding funding uplift
- supply chain impact: partners face repeated background checks and added costs for resilience obligations, which are priced into contracts
- funding constraints: fixed regulatory funding cycles make absorbing ongoing SOCI changes difficult, with grace periods often falling mid-cycle
- operational trade-offs: compliance efforts divert resources from operational priorities; some worry more time is spent on paperwork than improving security
- critical worker vetting costs: broad definitions and lack of alignment with existing standards (e.g., AusCheck vs AS4811) increase costs and duplication
- unplanned costs: organisations note lack of forward planning for SOCI-related expenses, creating financial pressure.

Q19 – The SOCI Act has introduced uncertainty or confusion around allocation of risk and responsibilities

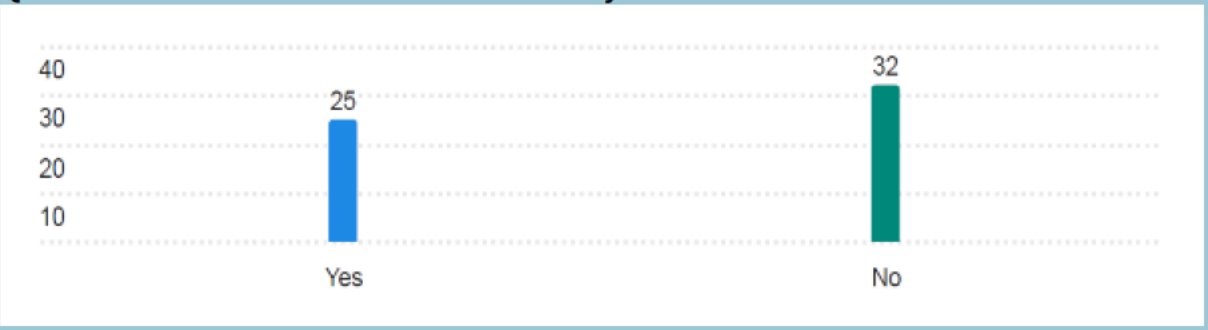


Figure 30: Bar chart for the responses to '*The SOCI Act has introduced uncertainty or confusion around allocation of risk and responsibilities*.

Q19(a) - If you answered 'Yes', please explain:

A summary of the responses provided is below:

- accountability and ownership ambiguity: unclear who is responsible for SOCI compliance—executive, legal, risk, or security teams—especially in multi-functional organisations
- cross-functional complexity: SOCI obligations impact multiple teams, requiring detailed RACI matrices and significant coordination effort
- supply chain risk allocation: difficulty enforcing SOCI requirements on suppliers; risk is not consistently passed through contracts, creating gaps
- unclear definitions and scope: ambiguity around what it means to "operate" certain components (e.g., third-party systems, data storage) and inconsistent interpretation of obligations
- sector and size disparities: smaller ISPs feel overburdened compared to larger carriers; unclear rationale for thresholds
- overlap with existing risk frameworks: SOCI compliance often perceived as administrative overhead rather than improving security posture
- governance shifts: risk teams taking ownership instead of security SMEs, causing misalignment in priorities
- operational challenges: increased workload, need for additional staff, and confusion in integrating SOCI obligations with existing enterprise risk programs
- positive step: formation of internal SOCI working groups has helped resolve some ownership and coordination issues.

Q20 - How effective is the SOCI Act's framework in supporting continuous improvement and uplift in critical infrastructure security?

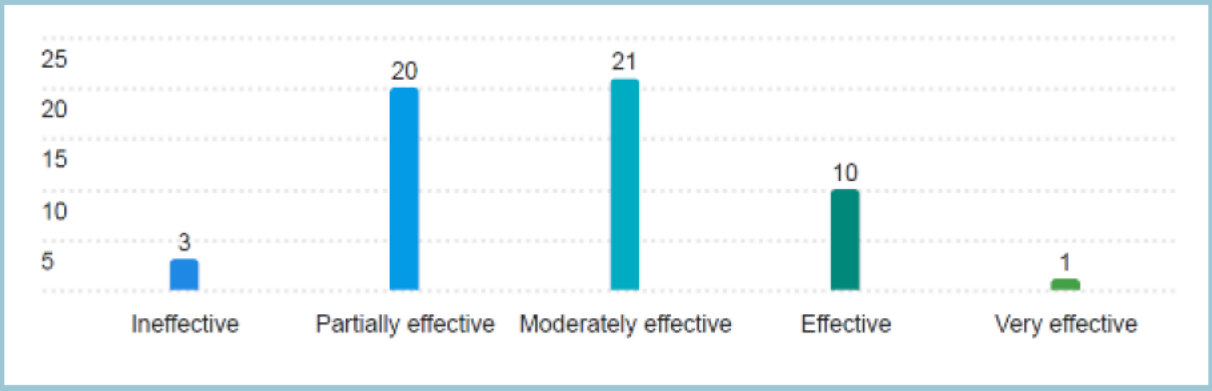


Figure 31: Bar chart for the responses to '*How effective is the SOCI Act's framework in supporting continuous improvement and uplift in critical infrastructure security?'*

Q21 - What are the main improvements you would recommend to ensure the SOCI Act remains fit-for-purpose?

A summary of the responses provided is below:

- raise the baseline and a tiered approach: current standards are too low for high-maturity entities; introduce tiered criticality levels and continually increase the bar for security maturity
- simplification and clarity: streamline processes, reduce legislative updates, and provide clearer definitions and practical examples of compliance expectations
- alignment and harmonisation: map SOCI obligations to existing frameworks (e.g., APRA CPS 230/234, PSPF, Essential Eight) to reduce duplication and complexity
- sector-specific guidance: provide tailored guidance for sectors like higher education, aviation, and OT environments; ensure industry-specific co-design for future changes
- improve personnel security processes: modernise background checks, allow recognition of alternative clearances, and strengthen guidance from CISC and AusCheck
- reduce administrative burden: consider bi-annual or for-cause reporting instead of frequent updates; simplify CIRMP reviews and reporting requirements
- funding and support: introduce funding mechanisms to help organisations invest in compliance and automation rather than paperwork
- enhance interdependency mapping: support exercises and tools to help entities understand and manage cross-sector dependencies
- clearer definitions for critical elements: define “critical worker,” “critical aviation asset,” and “data storage systems” more precisely to avoid ambiguity
- supply chain certification: implement standardised certification to streamline compliance in contractual arrangements.

Q22 - What additional guidance, tools or support would assist compliance?

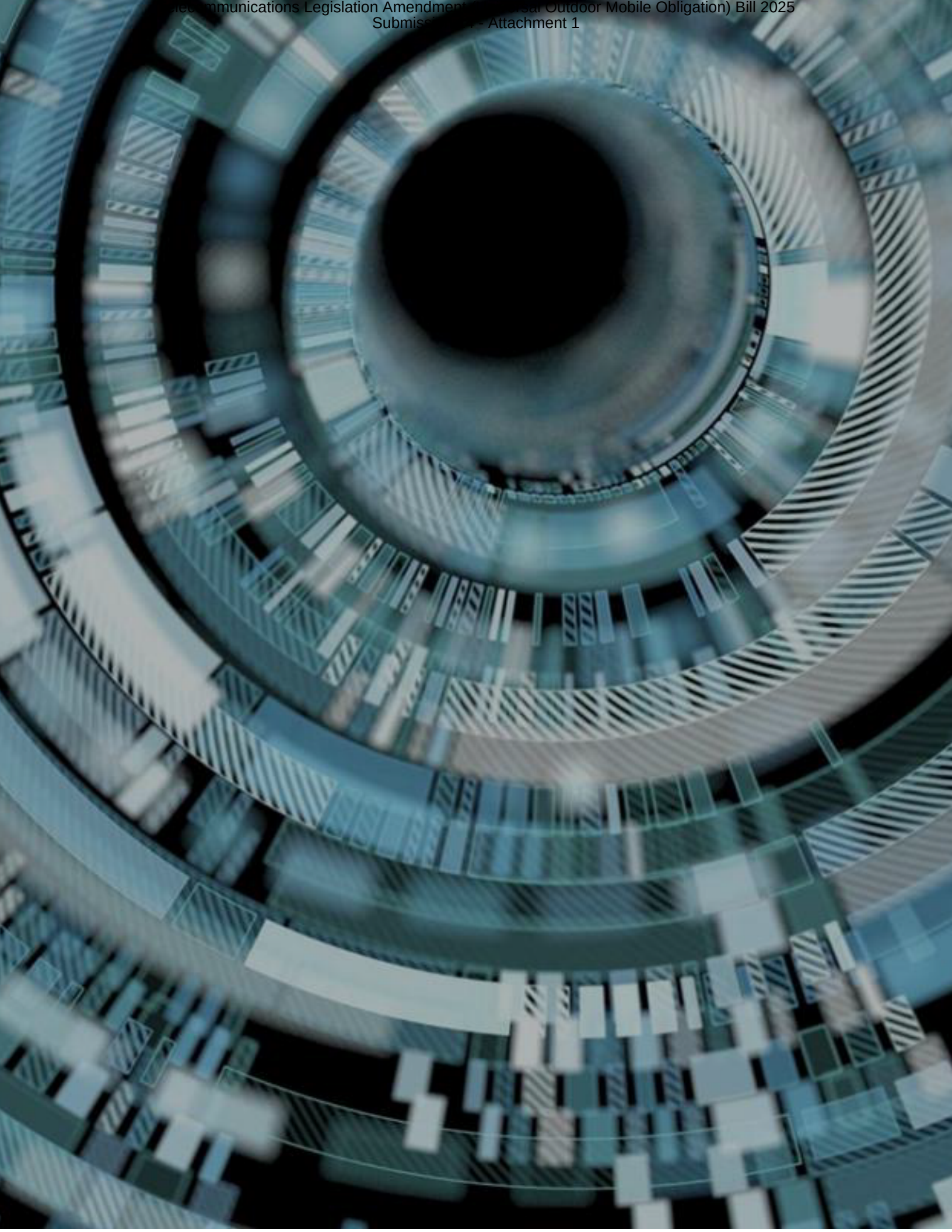
A summary of the responses provided is below:

- incentives for compliance: introduce additional incentives to encourage proactive compliance
- supply chain support: provide easy-to-use supply chain assessment tools and structured compliance frameworks for vendors
- board and executive engagement: develop more FAQs, guidance packages, and mandatory acknowledgment processes for boards to strengthen governance
- clear audit and maturity criteria: define expected standards/frameworks and provide maturity assessment tools
- industry-specific guidance: offer tailored guidance bridging SOCI obligations with sector-specific requirements; improve harmonisation across frameworks
- enhanced guidance and templates: simplify and centralise CISC guidance; provide templates for CIRMP, TSRMP, and attestation reports, especially for smaller ISPs
- training and education: deliver staff training materials, financial assistance for SOCI/CIRMP training, and educational resources on methodologies
- shared lessons and threat intelligence: share lessons learned from control failures and provide sector-specific threat intelligence to clarify risk likelihood
- improve accessibility of guidance: make CISC resources easier to navigate (filter by date, sector, obligation) and remove outdated materials promptly
- funding support: offer financial support for compliance activities and training to reduce burden on smaller entities.

APPENDIX J

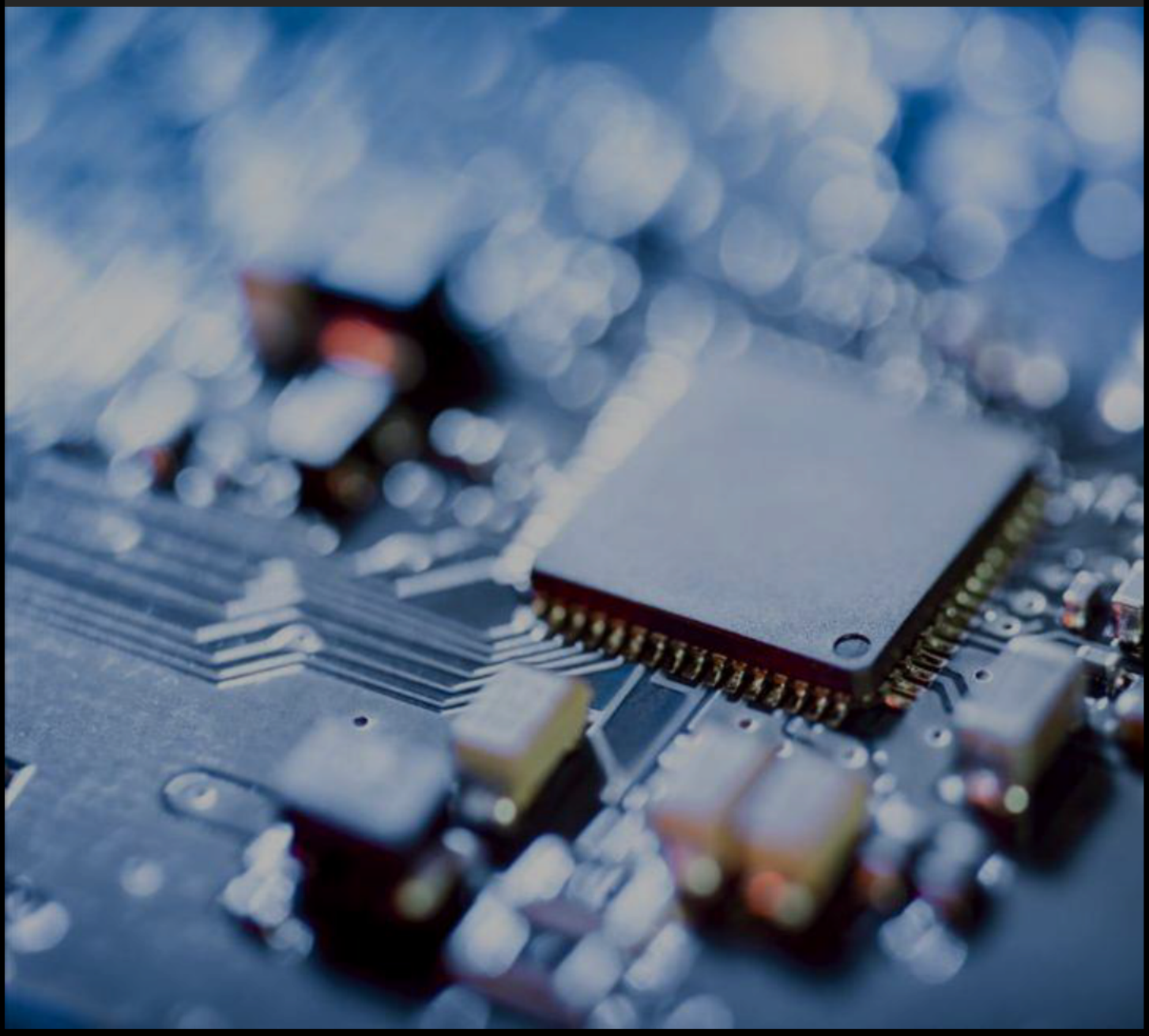
SECTOR-BY-SECTOR SOCI COMPLIANCE OBLIGATIONS AND SELF-ATTESTATION

Sector	Asset scope	Operator duties	Evidence expected



APPENDIX K

CYBERSECURITY AND CRITICAL INFRASTRUCTURE



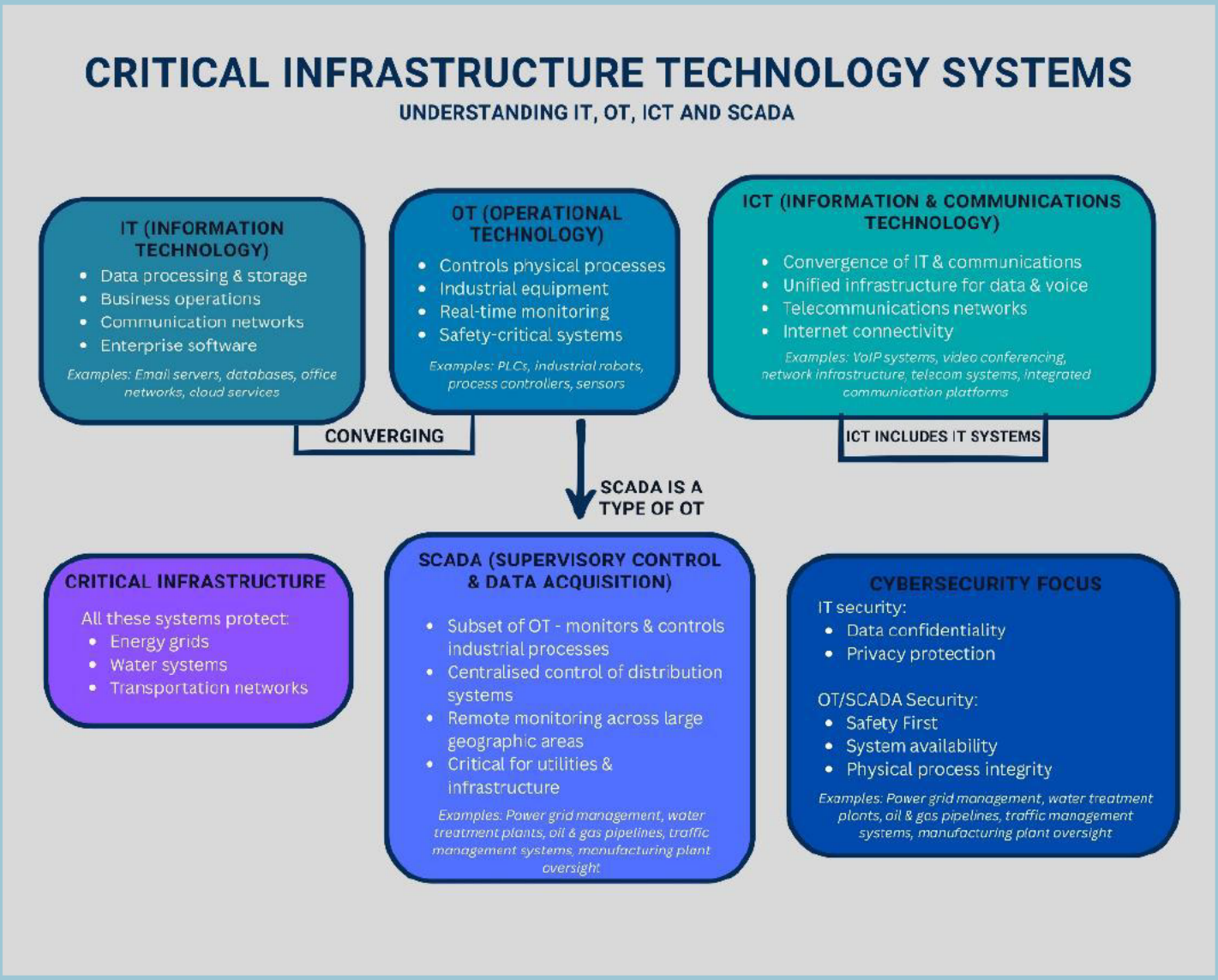


Figure 31: Critical infrastructure technology systems: understanding IT, OT, ICT and SCADA

All critical infrastructure has underpinning technology that controls it as part of its functionality. There is a large amount of discussion, as reported in this report, of the need (or lack of need) for a focus on cybersecurity as part of the risk management involved in the SOCI Act. An all-hazards approach is one where cybersecurity is just one factor, one element of risk, to be considered.

In an overarching sense the digital technology involved in critical infrastructure is generally labelled:

- IT (often based on Windows)
- ICT (IT systems which have an element of communications involved)
- OT controlling industrial equipment and physical processes. This might be the valves that operate in a water supply environment, switches of various kinds in telecommunications and electricity environments, or the systems that control physical operations. All of these Critical Technology Systems are vulnerable to disruption of a malicious or accidental nature
- SCADA (Supervisory Control and Data Acquisition systems). These generally control industrial processes and distributed systems.

Each of these critical infrastructure technology systems needs to be protected from cyber-attack and breach as well as all other hazards. A major reason for the SOCI Act risk management process is to provide the Minister

assurance that an entity can comply with a designated cybersecurity framework (including the AECSF) and meet specified maturity levels. This is discussed later.

OT systems are increasingly vulnerable to cyberattacks due to their unique architectural characteristics and operational constraints that differentiate them from traditional IT environments. The Purdue Model for ICS describes a hierarchical architecture where Level 0 encompasses the physical process layer (sensors, actuators, and field devices), which directly interfaces with industrial processes and often lacks built-in security features (Stouffer et al., 2023; Weiss, 2025a).

Weiss (2025a) emphasises that OT cybersecurity is fundamentally 'built on a foundation of sand' due to the absence of cybersecurity capabilities in Level 0 devices, which lack authentication mechanisms and have no inherent ability to detect cyber threats. OT systems are frequently compromised through inadequate network segregation between IT and OT zones, allowing attackers to pivot from corporate networks into critical control systems, a vulnerability exploited in high-profile incidents such as the 2015 Ukrainian power grid attack (Assante & Lee, 2015).

Additionally, OT environments face significant challenges with patch management due to the operational criticality of systems that cannot tolerate downtime, vendor-specific proprietary protocols, and legacy equipment that may be decades old without available security updates (Ginter, 2017). The absence of comprehensive logging and monitoring capabilities in many OT devices further compounds these vulnerabilities, as security teams lack visibility into anomalous activities and potential breaches (Weiss, 2024).

Traditional IT cybersecurity approaches often prove inadequate for OT environments because the fundamental priorities differ: while IT emphasises confidentiality, integrity, and availability in that order, OT prioritises availability, integrity, and confidentiality, as unplanned downtime can result in physical safety hazards, environmental damage, or massive production losses (Knapp & Langill, 2014). Standard IT security practices such as frequent patching, regular system reboots, vulnerability scanning, and network segmentation are difficult or impossible to implement in OT environments without disrupting critical operations that may run continuously for months or years (Stouffer et al., 2023).

Furthermore, many OT protocols were designed decades ago without security considerations, operating on the assumption of a physically isolated and trusted network environment, making them inherently vulnerable to modern cyber threats when connected to enterprise networks or the internet (Macaulay & Singer, 2011; Weiss, 2011).

Weiss (2024) argues that the organisational shift of OT cybersecurity responsibility to Chief Information Security Officers (CISOs), who traditionally managed enterprise IT security, has inadvertently worsened the problem, as IT-focused network security technologies and testing methodologies that work well in IT environments have "directly contributed to control system cyber-related incidents" when applied to OT systems without understanding their technical constraints. The convergence of IT and OT networks, driven by Industry 4.0 initiatives and remote access requirements, has expanded the attack surface while the specialised knowledge required to secure OT systems remains scarce among traditional IT security professionals (Ginter, 2017).

References

Assante, M. J., & Lee, R. M. (2015). *The industrial control system cyber kill chain*. SANS Institute. https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297

Ginter, A. (2017). *Industrial cybersecurity: Efficiently monitor the cybersecurity posture of your ICS environment*. Waterfall Security Solutions.

Knapp, E. D., & Langill, J. T. (2014). *Industrial network security: Securing critical infrastructure networks for smart grid, SCADA, and other industrial control systems* (2nd ed.). Syngress.

Macaulay, T., & Singer, B. L. (2011). *Cybersecurity for industrial control systems: SCADA, DCS, PLC, HMI, and SIS*. CRC Press.

Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., & Lightman, S. (2023). *Guide to operational technology (OT) security* (NIST Special Publication 800-82 Rev. 3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r3

Weiss, J. (2011). *Protecting industrial control systems from electronic threats*. Momentum Press.

Weiss, J. (2024, September 27). Sam Houston State University paper: "Who's in charge of OT security." *Control Global*. https://www.controlglobal.com/blogs/unfettered/blog/55143240/sam-houston-state-university-paper-whos-in-charge-of-ot-security

Weiss, J. (2025a, December 10). The need for appropriate Purdue Reference Model Level 0 cybersecurity training. *Control Global*. https://www.controlglobal.com/blogs/unfettered/blog/55337511/why-level-0-devices-require-dedicated-cybersecurity-measures

APPENDIX L

SUMMARY OF PUBLIC SUBMISSIONS

Theme	Key points	Supporting submissions	Divergent views	Consensus direction