Submission on the Security of Critical Infrastructure Act 2018 review

Rob Nicholls[1]

1 Summary

The SOCI Act has undergone substantial reform since its original enactment but contains significant blind spots that leave the nation exposed to emerging threats. In my view the critical gaps are that content delivery networks (CDN) and AI services fall outside the SOCI Act's explicit coverage, while space technology remains listed as a sector yet has no defined critical infrastructure assets.

These are all fundamental to modern Australian infrastructure but either fall outside the Act's explicit coverage or remain entirely undefined despite their sector listing. The June 2021 Akamai CDN outage disabled three of Australia's four major banks for four hours. Healthcare and financial decision-making have ongoing dependence on US-hosted AI services. These gaps are not theoretical concerns but operational vulnerabilities requiring immediate regulatory attention.

The SOCI Act framework has evolved through four major amendments between 2021 and 2024, including addressing gaps exposed by the Optus and Medibank breaches. However, this reactive approach was an *ex post* response rather than threat anticipation. This leaves Australia perpetually one step behind adversaries who have demonstrated both capability and intent to disrupt critical infrastructure.

2 The current SOCI framework and its structural limitations

2.1 Overview

The *Security of Critical Infrastructure Act 2018* (Cth), as amended and in force from April 2025, establishes a tiered regulatory framework across eleven sectors. These are: communications; data storage or processing; defence industry; energy; financial services and markets; food and grocery; healthcare and medical; higher education and research; space technology; transport; and water and sewerage (CISC 2024a). The Act imposes three positive security obligations on responsible entities: registration with the Critical Infrastructure Assets Register, mandatory cyber incident reporting (within 12 hours for

[1] Dr Rob Nicholls is a Senior Research Associate at the University of Sydney Centre for AI, Trust, and Governance.

significant impacts, 72 hours for relevant impacts), and maintenance of a Critical Infrastructure Risk Management Program covering cyber, physical, personnel, and supply chain hazards.

Assets declared as Systems of National Significance face enhanced obligations including incident response planning, cyber security exercises, vulnerability assessments, and provision of system information for real-time threat monitoring (CISC 2024b). Government assistance measures. This includes the controversial “step-in” powers, which allow ministerial direction and Australian Signals Directorate intervention as last resort mechanisms when entities are “unwilling or unable” to respond to serious incidents.

2.2 The definitional architecture creates coverage gaps

Each critical infrastructure asset class is precisely defined with technical thresholds. A “critical data storage or processing asset” must be a data centre with specific capacity or customer characteristics. The telecommunications sector covers carriers and carriage service providers. These bright-line definitions provide regulatory certainty but fail to capture novel infrastructure categories that didn’t exist when the definitions were drafted. The Act’s object clause references protecting infrastructure whose destruction or unavailability would “significantly impact the social or economic wellbeing of the nation”. This language is clearly applicable to CDNs, AI services, and satellite communications, yet these remain outside explicit coverage.

3 Content delivery networks: A single point of failure for Australian critical services

3.1 Overview

Content delivery networks have become invisible infrastructure underpinning virtually all internet-connected services in Australia (Huston, 2021). CDN-based traffic now exceeds non-CDN traffic globally, with 87.5% of the top 1,000 websites using CDN services (IO River 2024). The market is dominated by five US-headquartered providers: Akamai, Cloudflare, Amazon CloudFront, Fastly, and Microsoft Azure CDN. This concentration creates systemic vulnerability that Australian regulators have not addressed.

The June 17, 2021 Akamai outage demonstrated this risk in stark terms. A routing table value overflow in Akamai's Prolexic DDoS protection service triggered a four-hour disruption affecting approximately 500 global customers (CircleID 2021). These included Commonwealth Bank, ANZ, Westpac, St George, ME Bank, Macquarie Bank, the Reserve Bank of Australia, Virgin Australia, and Australia Post. The RBA was forced to cancel interbank market operations. Three of Australia's four major banks were simultaneously unreachable during business hours due to a single configuration error in Texas.

Eleven days earlier, the Fastly outage had caused similar global disruption, demonstrating these are not isolated incidents but predictable consequences of infrastructure concentration. When Fastly's network failed, some users of other CDNs were affected because those providers routed traffic through Fastly. This revealed "deep dependencies" that extend beyond obvious customer relationships (CircleID 2021).

3.2 CDN providers are not explicitly covered under current SOCI definitions

CDN providers may be indirectly captured if they qualify as telecommunications carriers or if they meet data centre thresholds, but pure-play CDN providers like Cloudflare, Fastly, and Akamai likely fall outside scope. The EU's NIS2 Directive, implemented October 2024, explicitly designates content delivery network providers alongside DNS providers, cloud computing services, and data centre operators as digital infrastructure subject to cybersecurity requirements (European Commission 2024a). The European Commission's implementing regulation specifically references CDNs, recognising that "CDNs have become a major part of the infrastructure of the modern internet".

Beyond operational risk, CDN dependence raises sovereignty concerns. All major providers are subject to the US CLOUD Act, which permits US law enforcement to compel disclosure of data stored on any server owned by US companies regardless of geographic location. CDN providers have also demonstrated willingness to terminate services based on content decisions. For example, Cloudflare's removal of protection from the Daily Stormer, 8chan, and Kiwi Farms might well be welcome in Australia. However, it establishes a precedent that Australian entities could face service denial based on US corporate policy decisions. There is no Australian-owned CDN provider of equivalent

scale to the US hyperscalers. While sovereign cloud and data centre options exist, CDN delivery remains substantially dependent on foreign infrastructure.

4 AI services: Critical infrastructure without coverage

4.1 Overview

Australia's dependence on overseas-hosted AI services presents a regulatory gap of growing urgency. Major AI providers, including OpenAI, Google, Microsoft, Amazon, and Anthropic, host their model inference infrastructure primarily in the United States. According to Security Brief Australia, "Most foundational AI model interactions (inferences) are not being processed in Australia. Our data is literally drifting offshore" (Sovereign Australia AI 2024).

This dependence spans critical sectors. The Commonwealth Bank has partnered with OpenAI for fraud detection (BankInfoSecurity 2024). Bendigo Bank is deploying Google's Gemini Enterprise. Over 10% of Australian adults used ChatGPT for health-related questions in 2024. The Reserve Bank of Australia warned in September 2024 that AI concentration among limited providers "may lead to higher correlation within markets" creating systemic financial risk (RBA 2024).

4.2 Service continuity is demonstrably unreliable

On December 26, 2024, Microsoft Azure's South Central US datacentre suffered a power failure that disabled ChatGPT, OpenAI's API, and related services globally for approximately nine hours. This affected Australian users during prime business hours. The July 2024 Azure OpenAI outage affected 14 of 28 regions including Australia East for nearly three days. StatusGator has tracked over 1,939 Azure OpenAI Service outages since monitoring began (StatusGator 2024).

AI services differ fundamentally from traditional cloud infrastructure in ways that magnify risk. Model weights represent proprietary intellectual property worth billions that cannot be substituted. Training data sources remain opaque, with Australian users having "zero visibility on how offshore models have been built". Switching between AI providers is not comparable to changing cloud vendors. Instead, each model has different capabilities, safety profiles, and integration requirements, creating effective lock-in.

The SOCI Act's data storage and processing sector provides no clear mechanism for capturing AI services hosted offshore. The EU AI Act, which entered force August 2024, classifies AI systems used in critical infrastructure as "high-risk" requiring conformity assessments, risk management, and human oversight (White & Case 2024). The US Department of Homeland Security published Safety and Security Guidelines for AI in critical infrastructure in April 2024. Australia has no equivalent framework, relying instead on voluntary AI Ethics Principles and hoping existing laws will suffice.

CSIRO has noted that "Without some degree of algorithmic sovereignty—the capability to produce or modify AI in Australia—the nation is exposed to new risks" (CSIRO, 2023). The Australian Academy of Science submission to the Productivity Commission identified that "Australia's ageing Tier-1 and Tier-2 HPCD facilities cannot meet escalating demand posed by AI" (AAS, 2025). Although there are projects to develop sovereign AI capability (including by fine tuning open weight models), no domestic alternative currently exists.

5 Space technology: A sector without defined assets

5.1 Overview

Perhaps the most striking gap in the current framework is the space technology sector. Space is explicitly listed as one of eleven critical infrastructure sectors under the SOCI Act. Yet according to the Cyber and Infrastructure Security Centre, "There are currently no critical infrastructure assets defined in the SOCI Act for the space technology sector" (CISC 2024c). The sector exists in legislation but has no operational content.

This gap exists despite Australia's rapidly growing satellite dependence. NBN's Sky Muster satellites serve over 400,000 remote Australian homes and businesses. Starlink has accumulated over 200,000 Australian subscribers and has been integrated into emergency services, fire trucks, police vehicles, and naval vessels. The NBN has announced plans to transition from its government-owned Sky Muster geostationary satellites to Amazon's Project Kuiper low-earth-orbit constellation by mid-2026. That is, replacing sovereign infrastructure with US corporate control.

5.2 The risks

Satellite cybersecurity vulnerabilities were demonstrated devastatingly by the Viasat KA-SAT attack on February 24, 2022, hours before Russia's invasion of Ukraine (Just Security 2022). Attackers exploited a misconfigured VPN appliance to deploy wiper malware that bricked 30,000 modems, causing what Ukrainian officials described as "huge loss in communications in the very beginning of war". Collateral damage included 5,800 German wind turbines losing remote monitoring and 9,000 European satellite internet subscribers (CyberPeace Institute 2022). Five Eyes nations including Australia formally attributed the attack to Russia's GRU.

The attack's success came through ground infrastructure rather than space-based components (Infosecurity Magazine 2022). Satellite ground stations, command and control facilities, teleports, user terminals,represent the primary vulnerability surface. Yet these facilities are not specifically defined as critical infrastructure under SOCI. GPS/GNSS dependencies pervade Australian critical infrastructure across aviation, emergency services, agriculture, and financial services timestamping, but no standardised processes exist for reporting, mitigating, or profiling positioning, navigation, and timing risks.

5.3 International approaches

The EU's NIS2 Directive designates the space sector as "essential" subject to the strictest cybersecurity requirements, covering ground-based infrastructure supporting space-based services, telecommunications operators, and satellite manufacturers (European Commission 2024a). ENISA published a comprehensive Space Threat Landscape Report in March 2025 with a 125-item cybersecurity control framework. The US has Space Policy Directive 5 establishing comprehensive cybersecurity policy for space systems and NIST frameworks specifically addressing satellite ground segment security. Australia has the Space (Launches and Returns) Act 2018 governing launches but nothing mandating satellite cybersecurity.

Starlink's dominance presents particular sovereignty concerns. Space Industry Association of Australia chief executive Dan Lloyd has noted that "Starlink has a track record of turning off services whenever something happens that Elon Musk doesn't like".

During Ukrainian military operations in Crimea, Starlink connectivity was disconnected following Russian communications with Musk. This demonstrates that foreign corporate decisions can "trump a country's sovereignty" over communications infrastructure.

6 Emerging threats outpacing regulatory response

Several threat categories have evolved faster than the SOCI framework can adapt.

6.1 Quantum computing

Quantum computing presents a cryptographic time bomb. The Australian Signals Directorate expects cryptographically-relevant quantum computers between the late 2020s and 2030s, with the Information Security Manual recommending phasing out vulnerable cryptography by 2030. State-sponsored actors are already conducting "harvest now, decrypt later" attacks. These intercept and store encrypted data for future decryption when quantum capability matures. Long-lived data including personal records, intellectual property, and government communications captured today may become readable within this decade. ASD has published a Post-Quantum Cryptography roadmap requiring completion of PQC transition by end of 2030, but this timeline imposes obligations the current SOCI framework does not enforce.

6.2 Supply chain attacks

Supply chain attacks have intensified dramatically. The SolarWinds compromise affected 18,000 organisations; the Log4j vulnerability touched millions of applications globally. Malicious open-source packages rose from 929 in 2020 to 459,070 in 2024. Australian incidents including the DP World Citrix Bleed exploit and Medibank contractor credential compromise demonstrate these attack vectors' effectiveness domestically. The SOCI Act requires supply chain hazard coverage in risk management programs, but provides limited mechanisms for hardware supply chain integrity or software bill of materials requirements.

6.3 Nation-state pre-positioning

Nation-state pre-positioning has reached strategic concern levels. The ACSC's 2024-25 Annual Cyber Threat Report documented a 111% increase in notifications to critical infrastructure entities of malicious activity. APT40 (China/Ministry of State Security)

“rapidly transforms and adapts exploit POCs within hours or days of public release”. Volt Typhoon (China/PLA) has been identified pre-positioning on power, water, and transport networks with the apparent aim of “disruption or destruction of critical services in event of geopolitical tensions or conflict”. ASIO Director-General Mike Burgess confirmed in November 2025 that China-linked hackers have “attempted to access Australia’s critical infrastructure, including telecommunications networks”.

6.4 Infrastructure interdependencies

Infrastructure interdependencies create cascade failure risks inadequately addressed by sectoral regulation. The November 2023 Optus outage affected 10 million mobile and internet customers. It cascaded to 400,000 businesses, government departments, Melbourne health and transport systems, and South Australia health and water services (Waterstons 2024). CSIRO’s Critical Infrastructure Protection Initiative found that “increasing digitisation within the construction and operation of critical infrastructure assets” creates new vulnerabilities where “even minor initial failures can transform into events of catastrophic proportions”.

7 International frameworks offer regulatory models

Comparative analysis reveals Australian regulatory gaps against peer jurisdictions.

The EU NIS2 Directive represents the most comprehensive approach, explicitly covering CDN providers, cloud computing services, data centre providers, managed service providers, and managed security service providers within its digital infrastructure scope (European Commission 2024b). It imposes 24-hour initial incident notification requirements, mandatory supply chain risk management, and penalties up to €10 million or 2% of global turnover. The Critical Entities Resilience Directive provides physical/operational counterpart coverage. The EU has also adopted the AI Act addressing AI in critical infrastructure and developed certification frameworks through the Cybersecurity Act.

The United Kingdom’s Cyber Security and Resilience Bill, introduced in November 2025, will bring data centres and managed service providers explicitly into regulatory scope with penalties up to £17 million or 4% of global turnover. It introduces critical supplier designation and 24-hour incident notification aligned with EU timeframes.

Canada's Bill C-26, passed December 2024, establishes the Critical Cyber Systems Protection Act with powers to prohibit high-risk equipment and suppliers, mandatory 72-hour incident reporting, and penalties up to $15 million for organisations (McMillan LLP 2024). It explicitly empowers vendor bans similar to the UK approach.

The United States has reaffirmed CISA as National Coordinator through National Security Memorandum-22 (April 2024), with proposed mandatory incident reporting within 72 hours and ransomware payment reporting within 24 hours. NIST Cybersecurity Framework 2.0 added a governance function and enhanced supply chain risk management. Executive Orders 14028 and 14144 impose software supply chain requirements including bills of materials and attestations.

Key patterns emerge from this comparison: explicit listing of digital infrastructure categories (not reliance on existing definitions); tiered obligations based on entity criticality and size; 24-hour initial incident notification becoming standard; direct management accountability for compliance; mandatory supply chain security provisions; and powers to ban high-risk vendors. Australia's SOCI framework incorporates some of these elements but lacks the explicit digital infrastructure coverage that defines contemporary international approaches.

8 Implementation experience reveals framework limitations

The SOCI Act's operational testing through major incidents has exposed both improvements and persistent gaps.

The Optus breach (September 2022) prompted Minister Clare O'Neil's assessment that the legislation was "bloody useless, not worth the ink printed on the paper when it came to actually using it in a cyber incident" (CVCheck 2022). The government lacked power to compel information sharing or direct cleanup activities once data had been exfiltrated. This direct experience drove the 2024 amendments expanding scope to data storage systems and enabling all-hazards response powers.

The DP World ports attack (November 2023) demonstrated improved coordination mechanisms. Declared a "nationally significant cyber incident," the response involved National Coordination Mechanism meetings co-chaired by the Cyber Security Coordinator with multi-agency participation. Operations resumed within three days.

However, the attack succeeded through an unpatched Citrix vulnerability. This is basic security hygiene that risk management programs should enforce.

Industry feedback indicates compliance burden remains substantial. The Australian Information Industry Association, while supporting the 2024 legislation "on balance," continues opposing expansion of Part 3A intervention powers as "broad in scope and unclear" (ARNnet 2024). Energy Queensland noted "much of the proposal duplicates existing cyber security regulations" and called duplication "both costly and unnecessary" (AEMC 2024). The domain name authority identified "cyber security rules and requirements developed in policy, regulatory, federal/state and departmental silos, resulting in duplication, dilution of efforts, and persistent legal uncertainty" (auDA 2023).

Multiple overlapping reporting obligations create particular friction: SOCI Act incident reporting (12-72 hours), Privacy Act Notifiable Data Breach scheme, APRA CPS 234 for financial services (72 hours for incidents, 10 days for control weaknesses), the new *Cyber Security Act 2024* (Cth) ransomware payment reporting (72 hours), and sector-specific requirements. Harmonisation remains incomplete.

The Cyber and Infrastructure Security Centre commenced full compliance audits in November 2024, signalling transition from education to enforcement. First annual CIRMP reports were due September 28, 2024. Trial audits conducted in 2023-24 inform the current compliance program (Tesserent 2024). However, the regulatory posture remains developmental; extensive consulting firm offerings on SOCI compliance indicate significant market demand for assistance navigating requirements.

9 Recommendations for reform consideration

In my view, there are several reform directions for consideration in the independent review:

Explicit digital infrastructure coverage should capture CDN providers, AI services, and managed service providers by name rather than relying on existing definitions. The EU NIS2 model of designating digital infrastructure categories provides regulatory certainty and addresses demonstrated gaps.

Space technology assets require Application Rules defining satellites, ground stations, and related systems as critical infrastructure. Ground segment security obligations should explicitly address the attack surface demonstrated by the Viasat incident.

Quantum cryptographic transition requirements aligned with ASD's 2030 deadline could be incorporated into CIRMP obligations for critical infrastructure handling long-lived sensitive data.

AI governance provisions addressing service continuity requirements, data sovereignty considerations, and human oversight for AI used in critical decision-making would begin addressing the regulatory vacuum identified by CSIRO.

Supply chain transparency including software bill of materials requirements and explicit high-risk vendor powers would align with international trends and address demonstrated attack vectors.

Regulatory harmonisation reducing overlapping reporting obligations while maintaining protection would address industry feedback on compliance burden without weakening security outcomes.

Cascade failure planning requiring cross-sector dependency mapping and resilience exercises would address the infrastructure interdependency risks highlighted by CSIRO and demonstrated by the Optus outage.

10 References

AAS 2025, Australian Academy of Science submission to the Productivity Commission on Australia's Productivity Pitch, Pillar 3: Harnessing data and digital technology file https://engage.pc.gov.au/document/540.

AEMC 2024, Energy Queensland Limited submission to AEMC, Australian Energy Market Commission, viewed 4 December 2024, https://www.aemc.gov.au/sites/default/files/2024-07/6%20Energy%20Queensland.pdf.

ARNnet 2024, 'Cyber legislation is a significant step in securing the nation's digital infrastructure: AIIA', ARN, viewed 4 December 2024, https://www.arnnet.com.au/article/3555188/cyber-legislation-is-a-significant-step-in-securing-the-nations-digital-infrastructure-aiia.html.

auDA 2023, Submission to the Department of Home Affairs: 2023-2030 Australian Cyber Security Strategy, .au Domain Administration, viewed 4 December 2024, https://auda.org.au/submission/submission-department-home-affairs-2023-2030-australian-cyber-security-strategy.

BankInfoSecurity 2024, 'Australian Bank Backtracks on AI-Led Job Cuts', BankInfoSecurity, viewed 4 December 2024, https://www.bankinfosecurity.com/australian-bank-backtracks-on-ai-led-job-cuts-a-29288.

CircleID 2021, 'The Deeper Root Cause of the Fastly and Akamai Outages', CircleID, 28 June, viewed 4 December 2024, https://circleid.com/posts/20210628-the-deeper-root-cause-of-the-fastly-and-akamai-outages.

CISC 2024a, Security of Critical Infrastructure Act 2018 (SOCI), Cyber and Infrastructure Security Centre, viewed 4 December 2024, https://www.cisc.gov.au/legislation-regulation-and-compliance/soci-act-2018.

CISC 2024b, Government assistance, Cyber and Infrastructure Security Centre, viewed 4 December 2024, https://www.cisc.gov.au/how-we-support-industry/government-assistance.

CISC 2024c, SOCI Act 2018 for space technology, Cyber and Infrastructure Security Centre, viewed 4 December 2024, https://www.cisc.gov.au/information-for-your-industry/space-technology/legislation-regulation-and-compliance/soci-act-2018.

CSIRO 2023, 'AI is already being used in healthcare. But not all of it is "medical grade" viewed 4 December 2024, https://www.csiro.au/en/news/all/articles/2023/june/ai-in-healthcare.

CVCheck 2022, '2022 SOCI Act amendments: What triggered the recent crackdown on data security?', CVCheck, viewed 4 December 2024, https://cvcheck.com/articles/2022-soci-act-amendments-what-triggered-the-recent-crackdown-on-data-security/.

CyberPeace Institute 2022, 'Case Study: Viasat Attack', CyberPeace Institute, viewed 4 December 2024, https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat.

European Commission 2024a, NIS2 Directive: securing network and information systems, European Commission, viewed 4 December 2024, https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

European Commission 2024b, Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) - FAQs, European Commission, viewed 4 December 2024, https://digital-strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive-faqs.

Huston G 2021, 'The CDN Conundrum', ISP Column, Potaroo, July, viewed 4 December 2024, https://www.potaroo.net/ispcol/2021-07/cdn.html.

Infosecurity Magazine 2022, 'Five Takeaways From the Russian Cyber-Attack on Viasat's Satellites', Infosecurity Magazine, viewed 4 December 2024, https://www.infosecurity-magazine.com/news/takeaways-russian-cyberattack.

IO River 2024, 'Who is the Largest CDN Provider?', IO River, viewed 4 December 2024, https://www.ioriver.io/questions/who-is-the-largest-cdn-provider.

Just Security 2022, 'AcidRain Malware and Viasat Network Downtime in Ukraine: Assessing the Cyber War Threat', Just Security, viewed 4 December 2024, https://www.justsecurity.org/83021/acidrain-malware-and-viasat-network-downtime-in-ukraine-assessing-the-cyber-war-threat/.

McMillan LLP 2024, 'Bill C-26: A New Chapter in Canadian Cybersecurity Regulation', McMillan LLP, viewed 4 December 2024, https://mcmillan.ca/insights/bill-c-26-a-new-chapter-in-canadian-cybersecurity-regulation/.

RBA 2024, 'Focus Topic: Financial Stability Implications of Artificial Intelligence', Financial Stability Review, Reserve Bank of Australia, September, viewed 4 December 2024, https://www.rba.gov.au/publications/fsr/2024/sep/focus-topic-financial-stability-implications-of-artificial-intelligence.html.

Sovereign Australia AI 2024, Sovereign Australia AI, viewed 4 December 2024, https://sovereign-au.ai/.

StatusGator 2024, Azure OpenAI Service Status, StatusGator, viewed 4 December 2024, https://statusgator.com/services/azure/azure-openai-service.

Tesserent 2024, Critical Infrastructure Resilience (SOCI Act), Tesserent, viewed 4 December 2024, https://tesserent.com/solutions/critical-infrastructure-soci-act.

Waterstons 2024, 'Cyber Incident Review', Waterstons, viewed 4 December 2024, https://www.waterstons.com.au/insights/latest-news/cyber-incident-review-3.

White & Case 2024, 'AI Watch: Global regulatory tracker - Australia', White & Case LLP, viewed 4 December 2024, https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-australia.