Australian Academy of Technological Sciences & Engineering

REPORT

FORTINET



Strengthening the resilience and integrity of Australia's critical operational systems

Securing the systems of modern Australian life.

NOVEMBER 2026

Australian Academy of Technological Sciences & Engineering

Strengthening the resilience and integrity of Australia's critical operational systems

Securing the systems of modern Australian life

Independence statement
This report was prepared by ATSE in partnership with Fortinet, the project's sponsor, and independently peer-reviewed before publication. The work was overseen by a Steering Committee of Academy Fellows and Fortinet representatives.
The report assesses no products or vendors.

Use of generative AI
Generative AI was used in the drafting and editing of the report under the supervision of senior researchers. The research, ideas, analysis, findings and recommendations in this report are the original work of its authors.

Project Team
Harry Rolf – Managing Director, Shape Policy
Nicola Smillie – Policy and International Projects Manager, ATSE
Olivia Allen – Lead Policy Analyst, ATSE

Strategic communications, design and production
Adam Huttner-Koros – Communications and Campaigns Manager, ATSE
Dan Wheelahan – Media & Reputation Manager, ATSE
Elizabeth Geddes –Brand & Digital Manager, ATSE

Review
Dr Cathy Foley AO PSM FTSE FAA
Kelly Bayer Rosmarin FTSE
Dr Ian Opperman FTSE

Citation
Australian Academy of Technological Sciences and Engineering, *Strengthening the Resilience and Integrity of Australia's Critical Operational Systems: Securing the systems of modern Australian life* (2026).

DOI Digital Object Identifier
https://doi.org/10.60902/q603-mm87

Acknowledgements
With thanks to the Steering Committee, chaired by Kelly Bayer Rosmarin (Appendix A), to the practitioners and strategic experts who took part in interviews and to the experts who responded to the survey.

We acknowledge Traditional Owners of Country across Australia and recognise their continuing connection to land, water and community. We pay respect to Aboriginal and Torres Strait Islander culture, and Elders past and present.

ABOUT ATSE

The Australian Academy of Technological Sciences and Engineering (ATSE) is a Learned Academy of independent, non-political experts helping Australians understand and use technology to solve complex problems. Bringing together Australia's leading thinkers in applied science, technology and engineering, ATSE provides impartial, practical and evidence-based advice on achieving sustainable solutions and advancing prosperity.

ABOUT FORTINET

Fortinet is a driving force in cybersecurity, delivering integrated protection for digital and operational systems that people, economies and communities rely on. The Fortinet Security Fabric combines secure networking, Unified SASE and security operations in an AI-powered platform, improving visibility and coordinating protection, detection and response across IT, OT and cloud. Trusted by over one million customers, Fortinet strengthens resilience through the industry's largest integrated cybersecurity portfolio, threat intelligence and collaboration with government, industry and academia.

Table of contents

Executive Summary **6**

Introduction **18**
- Australia's critical operational systems 20
- A systems perspective 20
- Emerging challenges facing critical infrastructure 22
- What resilience means for critical operational systems 23
- Australia is adapting to emerging challenges 24
- What the rest of this report does 25

Defining Australia's critical operational systems **26**
- What the law counts as critical 26
- How the SOCI Act assesses what is critical 27
- Why an asset-based definition does not answer a dependency question 28
- What government says about interconnection, and what it measures 29
- What this means 29

The cyber threat landscape **30**
- What the national in cident picture shows 30
- Information technology and operational technology are no longer separate 31
- Exposure is increasing 32
- Attacks are increasingly aimed at disruption 33
- The pathway runs through the supply chain 34
- What this means 34

Systemic vulnerabilities in Australian critical systems **36**
- Interdependency 36
- Concentration 38
- Fragmented governance 38
- Colliding obligations 40
- Supplier risk 40
- Privileged access 41
- Legacy infrastructure 42
- Capability 42
- What this means 43

The policy and regulatory landscape **44**
- How others regard the Australian model 45
- What the review found, and what is being done 45
- What has not been measured 46
- The remaining gaps need more than regulation 46

Building national resilience **48**
- Building on Australia's regulatory foundation 48
- From critical assets to critical systems 48
- Building capability through practice 48
- Assigning responsibility for the system 50
- Applying existing approaches nationally 50
- Building national resilience 51

Appendices **52**

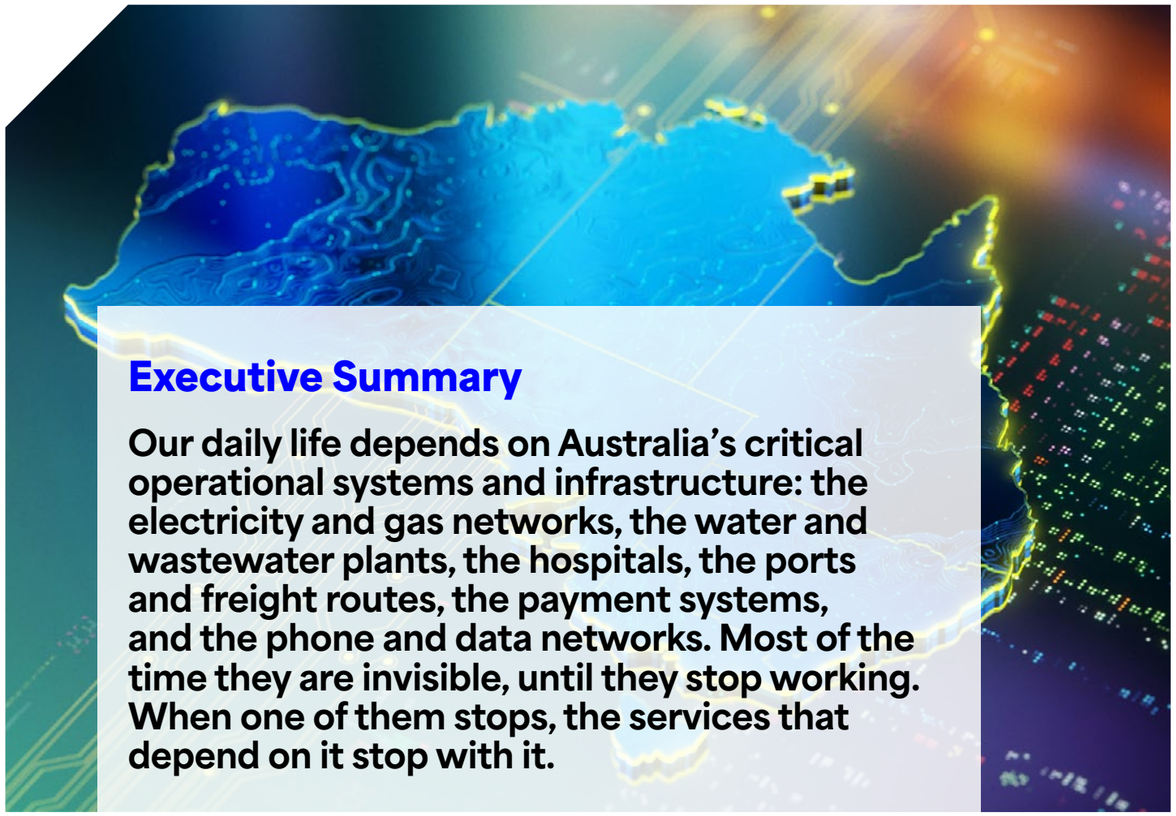
Appendix A: Steering Committee 52

Appendix B: Literature review 53
- Search strategy 53
- Evidence base 54

Appendix C: Survey 55
- Which systems matter, and why 55
- Threats, and which are underestimated 55
- Vulnerabilities 56
- Governance, and confidence in the policy settings 56
- What respondents would do 57
- What is overlooked 57
- How the report uses these results 57

Appendix D: Interviews 58
- Interconnection and the limits of isolation 58
- Legacy systems and the pace of change 59
- Governance, ownership and skills 59
- Standards, guidance and coordination 60
- AI and dependence 61
- Research and domestic capability 62
- What interviewees would change 62
- How the report uses these findings 62

Endnotes **64**



Executive Summary

Our daily life depends on Australia's critical operational systems and infrastructure: the electricity and gas networks, the water and wastewater plants, the hospitals, the ports and freight routes, the payment systems, and the phone and data networks. Most of the time they are invisible, until they stop working. When one of them stops, the services that depend on it stop with it.

THIS REPORT EXAMINES the cyber security of these interconnected systems. It asks how the systems depend on one another, how a disruption in one spreads to others, where responsibility for that risk sits, and what it takes to keep the systems running.

Cyber threats and policy settings are both changing. Australia's incident data shows attacks on critical infrastructure increasingly aimed at making services unavailable.[1] The connection between information technology (IT) and operational technology (OT), once kept separate, now provides a route for attack. Half of all vulnerabilities analysed by the Australian Signals Directorate (ASD) were exploited within two weeks of a fix being released,[2] and artificial intelligence (AI) is shortening that interval further.[3] ASD reports that state-sponsored actors routinely target critical infrastructure networks, possibly to pre-position for disruptive effect in a crisis.[4,5,6]

This report is written for policymakers and the people who run critical operational systems and infrastructure. For the Australian Government, and for the states and territories, it provides independent evidence to inform the reform of the *Security of Critical Infrastructure Act 2018* (SOCI Act) now under way following its independent review in early 2026, and an assessment of how well the reforms address the risks it identifies. For the boards, executives and engineers who operate critical infrastructure, and for the suppliers who build and support it, it sets out where the risk now sits and how that risk can be managed within existing arrangements.

This report was prepared by the Australian Academy of Technological Sciences and Engineering (ATSE) in partnership with Fortinet and overseen by a Steering Committee of Academy Fellows and Fortinet representatives (Appendix A). It draws on a review of current published literature, a survey of 36 experts from research, industry and government, and interviews with practitioners and strategic experts.

What the report finds

Australia regulates critical infrastructure comparatively well. The independent review found the SOCI Act had established Australia's leadership in critical infrastructure security governance.[5] New Zealand's 2026 discussion document, for example, places Australia among the five jurisdictions New Zealand looked at when developing its own regime.[7] The review also identified complexity, regulatory overlap, a weak enforcement posture and gaps in addressing emerging threats.[5] Responses to the review's criticisms are under way: enhanced risk management program rules were made in June 2026, and a broader reform package was released for consultation.[8,6]

This report identifies six issues that go beyond the SOCI Act reforms:

- Dependencies between critical systems are often unknown.
- Operators are responsible for securing equipment and services they did not build.
- The capability to manage risk across operations, IT and governance is scarce and unevenly spread.
- Information can become stuck when it is needed most.
- Whether resilience is improving is not yet measured.
- Digital and AI infrastructure is not yet recognised as critical.

Addressing these issues requires shared information, practice and capability across operators, which regulation on its own does not create. Additionally, two conditions run through all six issues: Convergence, where equipment that was once secured by isolation is now connected to corporate networks and through them to the internet, and Interdependency, where a service failure also disrupts the services that depend on it, so the consequence of a failure is set by what relies on the system, whatever the size of its operator.

Each issue is presented below with the finding that supports it and a series of recommendations for how it can be addressed. The recommendations build on the regulations, the strategy and the networks Australia already has in place.

ISSUE 1

Dependencies are often unknown

Cascading failure, where the loss of one service disrupts the services in other sectors that depend on it, is identified as one of the most consequential risks to Australia's critical infrastructure.

The ***Annual Risk Review*** of the Cyber and Infrastructure Security Centre (CISC) states that significant disruption in one sector will affect others.[9] Current reforms to the SOCI Act propose to address this risk by giving the dependencies between infrastructure more weight in determining what is critical.[6,10] However, a holistic national view of these dependencies is not publicly available. The states of Victoria and Queensland have assessed dependencies across sectors within their borders,[11,12] and the CISC asks each sector to consider cascading effects.[13] But a national assessment that brings this state and sector work together, and includes cyber risk, is not publicly available. Operators also have a limited view of their own dependencies. Queensland's Auditor-General found that the entities it tested could not describe their direct third-party exposure.[14] Australia would benefit from a national assessment of critical infrastructure dependencies, and the methods to assess cascading risk are already available.

RECOMMENDATION 1

Create a national assessment of Australia's critical infrastructure dependencies, share it regularly with the governments and operators who need it, and establish clear responsibility for its ongoing delivery.

a. The Australian Government should establish a national assessment of critical infrastructure dependencies, built with the states and territories from the cross-sector material they already produce, the CISC's sector risk advisories and risk assessments, and the work of the Trusted Information Sharing Network (TISN) sector groups, and covering cyber alongside other hazards. The assessment should support planning, be developed with operators, and be repeated as systems change. Systems of National Significance (SoNS) already identify the most consequential assets and attach enhanced obligations to them. A national assessment would add a view of the services that this infrastructure supports, across assets, sectors and jurisdictions. It would show which services depend on each system, whether alternatives or substitutes are available, how quickly disruption could move between systems, the order in which services would need to be restored, and the consequences for communities and other operators.

b. In Australia the SOCI Act does not address risks that sit between entities, where a failure at one operator disrupts the services of another. To address these risks, responsibility for the resilience of Australia's critical infrastructure system should be given to a named minister and agency. New Zealand's 2023 Cabinet paper proposed something similar for its own regime.[15] In practice, the Minister for Home Affairs and the CISC already administer the SOCI Act and support delivery of the *Critical Infrastructure Resilience Plan*, and would be the appropriate holders of this responsibility.[16] The mandate would also cover keeping the proposed national dependency assessment current, coordinating restoration priorities across sectors, and reporting on the outcome measures in Recommendation 5.

c. Sector-level resilience assessments should be considered for the priority sectors of communications, energy, health, transport and water, and connected into the proposed national dependency assessment. The telecommunications profile prepared by the Australian National University's Tech Policy Design Centre (TPDC) offers one potential approach to consider.[17]

d. The supply chain mapping that the *Security of Critical Infrastructure Legislation Amendment (Enhanced Critical Infrastructure Risk Management Program) Rules 2026* require of nine specified classes of asset[8] should feed the national dependency assessment. The national assessment should be returned to operators so that an entity can see what depends on it and what it depends on. Access should be limited to the governments and operators involved, because a national picture of where failure travels furthest would also be useful to an attacker.[15] The reform program should use that evidence when it decides what is critical.



Cascading failure, where the loss of one service disrupts the services in other sectors that depend on it, is identified as one of the most consequential risks to Australia's critical infrastructure.

ISSUE 2

Operators are responsible for equipment and services they did not build

Most equipment that runs physical processes was engineered for safety and long life in an era when it was not able to communicate with anything: the equipment often cannot be patched, taken offline or replaced without stopping the service; controls designed for office computing can be harmful when applied to industrial equipment; and disconnection is not available either, because vendors that supply this equipment need access for as long as it is in service.

In general, an operator can have strong internal controls and still be exposed through the products it buys, the vendors and services it relies on and the access it grants suppliers.[6] The Act places the obligation to manage that risk on the operator.[10] The design decisions that created that risk were often made by the vendor at the time of construction. Cloud and AI services carry the same dependency for every sector. Access to leading AI models has been interrupted before.[18]

RECOMMENDATION 2

Make protection between systems the expectation, and support operators and suppliers to share responsibility for the security of what is sold and supported.

a. Segregation that keeps a service running when a connected system is compromised should be taught, encouraged and evaluated in testing across regulated sectors, building on the *Security of Critical Infrastructure Legislation Amendment (Enhanced Critical Infrastructure Risk Management Program) Rules 2026* for nine specified classes of asset.[8] When ransomware reached CS Energy in 2021, segregation kept generation running.[19] Simple and visible controls, such as a manual authorisation step on vendor remote access, should be promoted in guidance, because operators and regulators can both see them work.

b. Australia should consider the adoption of internationally recognised OT security standards, such as the ISA/IEC 62443 family,[20] because they set out who is responsible for security at each stage of an asset's life, from product supplier to asset owner. The enhanced risk management program rules require the responsible entities for nine specified classes of asset to comply with one of five listed cyber frameworks, or an equivalent, and none of the five is specific to OT.[8] Government should consider adding ISA/IEC 62443 to that list. Practitioners interviewed asked for guidance that helps them prioritise among the standards they already work to (Appendix D). Agencies and operators should use the standards already in place before developing new processes. International guidance continues to develop, including the draft fourth revision of the United States National Institute of Standards and Technology guide to OT security, released for comment in September 2026.[21]

c. Supplier obligations are set at procurement, which the report finds is often a decision led by people without cyber and critical infrastructure expertise. Procurement guidance for critical infrastructure should expect supplier conformance to recognised standards and secure-by-design commitments, and should help small and medium enterprises in supply chains meet those expectations.

d. The reform program proposes a new category of relevant operator,[6] so that third parties with material practical control over an asset carry obligations for it.

ISSUE 3

Capability across operations, IT and governance is scarce and uneven

Resilience in OT environments, the plants, networks and control rooms that run physical processes, requires people who understand industrial operations, IT and the governance expectations that surround both.

That capability now spans AI as well. Few people have expertise across all these areas, so risk that crosses the boundary between an operations team and an IT team, or between an operator and its regulator, can fall between them. The Australian Strategic Policy Institute (ASPI) finds that boards frequently lack the expertise to interrogate OT cyber risk, and survey respondents named attestation without a technical basis among the most significant vulnerabilities in Australia's critical systems (Appendix C).

The ***Critical Infrastructure Annual Risk Review*** reports that training, capability and retention pathways are insufficient to meet demand, with the shortage most acute in engineering and maintenance, cyber security and automation.[9] A representative account of the OT security workforce was not identified. Smaller and regionally critical operators have the least capability and the fewest alternatives when something fails. Where audited entities gave reasons for missing minimum requirements, the most common were uplift programs still in progress and budget,[23] indicating a resourcing problem. Interviewees described technical capability in government as uneven and said hiring and clearance arrangements often make it harder to bring technical expertise in (Appendix D).

RECOMMENDATION 3

Build capability where operations, IT and governance meet, and support the operators least able to build it alone.

a. Boards of responsible entities already approve the annual risk management report under the SOCI Act.[10] That approval should be supported by an assessment from an appropriately qualified expert, as the independent review proposed,[5] and boards should have access to capability spanning IT, OT and AI, through training, advisers or appointments. Appointments should aim to place the right expertise in the positions that need it. A named executive accountable for AI risk, which ASD recommends,[24] or a chief AI officer, is one approach to consider. Government and industry bodies should provide the training and the shared advisers that are beyond the budget of smaller entities.

b. Government should publish guiding principles that help operators prioritise, alongside the regulatory guides with worked examples the independent review recommended,[5] and should facilitate the sharing of practice between operators. Government agencies should build awareness of existing standards and use them before developing new processes, including for AI.

c. Support for smaller and regionally critical operators should be organised as shared capability: central technical expertise they can call on before and during an incident, as some states provide, and a domestic equivalent of the cyber security uplift grants Australia funds abroad (Appendix C).

d. Economic regulators should account for future cyber risk alongside historical benchmarks, so that an operator whose revenue is set by one regulator can fund an obligation set by another.

e. Regulators and policy agencies should hold technical capability alongside policy capability, including in senior roles. Government should be able to use mechanisms such as the *Australian Public Service Mobility Framework* and secondments from industry and research to bring technical expertise into senior teams and should review the hiring and clearance arrangements to ensure they support this (Appendix D). Engagement between the people who operate these systems and the people who set rules for them should be supported.

f. Australia funds research on securing these systems but, in interviewees' experience, has no dedicated route from that research to deployed capability (Appendix D). Critical infrastructure protection should be a distinct research and commercialisation priority, with a pathway for applying Australian research to the design, security and deployment of systems.



Resilience in OT environments requires people who understand industrial operations, IT and the governance expectations that surround both.

ISSUE 4

Information can become stuck when it is needed most

Incident information serves three purposes during an incident: first, reporting the incident to government; second, warning other operators, in time and in enough detail to act on; third, telling the public what is happening and what to do.

The SOCI Act provides for the first.[10] Warning other operators and informing the public depends on arrangements outside the Act. Threat sharing was seen to work well where it exists. Interviewees described the anonymised national threat intelligence capability as a strength, and said one sector coordinates effectively because regulation gave it a coordinating centre and made clear that competitors may work together (Appendix D).

Public communication during major outages is a known issue. The review of the 2023 Optus outage found the public could not be told what was happening because the fault could not be seen clearly, and the CISC's sector risk advisories describe disinformation as a tactic that can be used to erode trust and disrupt communication.[13] Victoria's critical infrastructure sectors list misinformation and disinformation among their emergency risks.[11] Laws can also conflict. A listed entity's continuous disclosure obligations can require public disclosure of an incident before it is contained.[26] During an attack, early public disclosure can alert the attacker and disrupt remediation being coordinated with ASD.[26] No clear arrangements for sharing assessments of AI and other emerging technology risks were identified in the preparation of this report.

RECOMMENDATION 4

Give operators permission and the means to share information and experience on cyber incidents in critical infrastructure, and build a shared way to assess AI and emerging technology risks.

a. Each sector would benefit from having a body whose role is to receive incident reports, share intelligence across sectors and with overseas counterparts, and pass it to operators in a form they can act on, including operators without the capability to take in government threat feeds directly (Appendix D). Survey respondents pointed to the arrangement in banking as the model (Appendix C), and the TISN sector groups would be a base to build from.[27] Government's role should be to give each sector its coordinating centre and explicit permission for competitors to cooperate, with the protection that lets an organisation work with ASD during an incident. ASD should lead the national layer of this sharing through its Cyber Security Partnership Program and its Cyber Threat Intelligence Sharing service, which interviewed practitioners valued (Appendix D).[2]

b. Government and industry bodies should convene regular practitioner forums, held under the Chatham House Rule, where operators can describe the measures they have taken, what happened and what did not work, so that other operators can learn from that experience (Appendix D). Forums should be secure enough to hold the trust of participants. Government's convening role should be defined and funded separately from its regulatory role. Sharing should cover threats, risks and solutions. Operators should remain free to take different approaches, because variety across operators limits how far a single fault or attack can reach.

c. Public communication during disruption should be treated as part of resilience and planned for. The Bean review of the Optus outage and the Triple Zero inquiry provide the starting evidence. Operators of designated assets should include public communication in the exercises they run, and test whether they can see a fault well enough to describe it. The exercise program of the Australian Cyber Security Centre (ACSC) already tests communications capability with operators,[2] and should extend this testing to public communication during outages. The arrangements for public communication during an attack, including who decides what is said and when, and for countering false information, should be settled in advance between operators and government, and research on what works should be commissioned.

d. The Department of Home Affairs' 2026 consultation paper proposes a power for the Minister to direct an entity not to disclose an incident, which would enliven an exemption from the Australian Securities Exchange (ASX) listing rules, with a limit of 120 days and insider trading controls.[28] The report notes the proposal, which would resolve a collision the Department itself identified, between continuous disclosure obligations and the risk that early disclosure alerts the attacker and disrupts remediation. Safeguards for market integrity are a matter for the Department, the Australian Securities and Investments Commission (ASIC) and Treasury.

e. Government, through ASD and the CISC, should develop with operators a shared framework for assessing AI and other emerging technology risks to critical infrastructure, including quantum computing. The framework should help an organisation judge whether a risk is real for its own systems and what response is proportionate. It should build on existing guidance, including the joint principles for the secure integration of AI in OT,[29] the CISC's factsheet on AI in critical infrastructure[30] and ASD's guidance on AI-enabled attacks.[24] It should also cover the data AI systems rely on, including where privacy and critical infrastructure obligations meet.

ISSUE 5

Whether resilience is improving is not yet measured

Australia can describe its critical infrastructure regime in detail. The regulator received 457 annual reports covering 831 assets in 2023-24, each approved by the entity's board,[31] and the risk management program obligations were costed at about $1.1 billion a year.[32]

No Australian source measures whether outages have become shorter, recovery faster or cascading failures rarer since the obligations commenced. Some independent testing is undertaken. Audit offices in Queensland, Western Australia and Victoria have tested public sector cyber controls and found weaknesses in each case,[14,70,72] and the Australian National Audit Office (ANAO) found that a department which had assessed itself as meeting the required standard did not meet it for seven of eight strategies. This testing is scattered across jurisdictions, covers a handful of entities at a time, concerns office systems more often than OT, and is aimed at government bodies. Meanwhile, national evidence from regulated entities consists mainly of self-assessments. The Department of Home Affairs states that regulator-led audits cannot provide broad assurance across the regulated population, and proposes independent assurance at least once every three years.[6]

RECOMMENDATION 5

Measure resilience against service outcomes, and bring the testing that already happens into one national view.

a. The Australian Government should define the outcomes the regime is intended to produce, measured by outage duration, recovery time and the frequency of cascading failure, and collect the evidence to measure them across the regulated population. The United Kingdom's *Cyber Assessment Framework*[34] offers one approach to consider for converting resilience principles into assessable outcomes.
b. The proposed independent assurance should assess whether controls operate under the pressure of an incident, including in OT, and an entity's attestation should be supported by a technical assessment.
c. The adversarial testing of the audit offices, Victoria's exercise and audit regime for designated operators under Part 7A of its *Emergency Management Act 2013*,[35] and the ACSC exercise program should be brought into one national view of what has been tested and what was found. Testing should extend to regulated private operators, through the proposed independent assurance or through an extended audit mandate.
d. Exercises should run through to recovery, with the people who would implement the plan, and should include OT scenarios, executive decision-making, and how last-resort powers would work in practice.
e. Any national application of resilience frameworks should define its intended outcomes at the outset and collect the evidence to evaluate whether the framework worked. The evidence reviewed for this report does not show whether applying them has prevented outages or improved recovery.

ISSUE 6

Digital and AI infrastructure is not yet recognised as critical

Every sector this report covers now depends on digital and AI infrastructure. Communications, energy, health, transport and water run on data centres, cloud services and AI compute, and interviewees described people in operational settings acting on machine-generated advice (Appendix D).

That dependence is concentrated. Three providers earned about 82% of Australian infrastructure-as-a-service revenue in 2023,[36] and interviewees described a small number of AI models, trained in similar ways, sitting beneath a growing number of systems (Appendix D). A fault in one cloud region or one widely used model could therefore disrupt several sectors at once. Access is a further risk, and interviewees noted periods when access to leading models was restricted.[18]

The SOCI Act recognises part of this layer. Data storage or processing is one of its eleven sectors,[10] and the reform program proposes to name large data centres and major cloud providers as critical infrastructure in their own right.[6] Space-based services are in a similar position. Most critical infrastructure sectors depend on satellite communications or positioning, navigation and timing.[9] Space technology has been a named sector since 2021 without practical effect, and the reform program proposes its first operative asset classes.[6] However, neither the current nor the proposed definition names AI compute or the providers of AI models.[6] The independent review recommended that coverage of AI infrastructure and services be examined.[5] Other jurisdictions already treat this layer as critical. The United Kingdom designated data infrastructure as Critical National Infrastructure in September 2024,[5] and the European Union's second Network and Information Security Directive (NIS2) lists data centres and cloud services among its highest-criticality sectors.[37] Recognition would also bring this layer within reach of government support in a serious incident, and into national planning and investment. Planning for national compute is still developing, and the Australian Academy of Science reported in 2025 that Australia does not yet have a plan for the next generation of supercomputing.[38]

RECOMMENDATION 6

Recognise digital and AI infrastructure as critical, in regulation and in national planning and investment.

a. This report's findings support the Department of Home Affairs' 2026 proposal to name large data centres and major cloud providers as critical infrastructure under the SOCI Act, and its proposed asset classes for space technology. As the independent review recommended, the Australian Government should also examine coverage of AI compute and of the providers of the AI models that critical infrastructure depends on. That examination should establish which critical services rely on these providers, and what obligations and support should apply to them. The definition of digital infrastructure should name data centres, cloud services and AI compute alongside the networks that connect them, and should state how it relates to the communications sector, which already covers telecommunications.

b. Recognition should bring support as well as obligations. Assets covered by the SOCI Act are within reach of government assistance in a serious incident.[10] Recognition should apply the three steps this report proposes for every sector: define what is critical, map what depends on it and assign responsibility for its resilience. It should also bring digital and AI infrastructure into national exercises and incident support.

c. The Australian Government and Infrastructure Australia should plan and fund digital and AI infrastructure, including national supercomputing, as long-term national infrastructure alongside energy, water and transport, because every critical infrastructure sector now depends on digital and AI infrastructure. The Australian Academy of Science has called for a long-term national strategy for high-performance computing and data,[38] and ATSE has set out investment options for national AI compute.

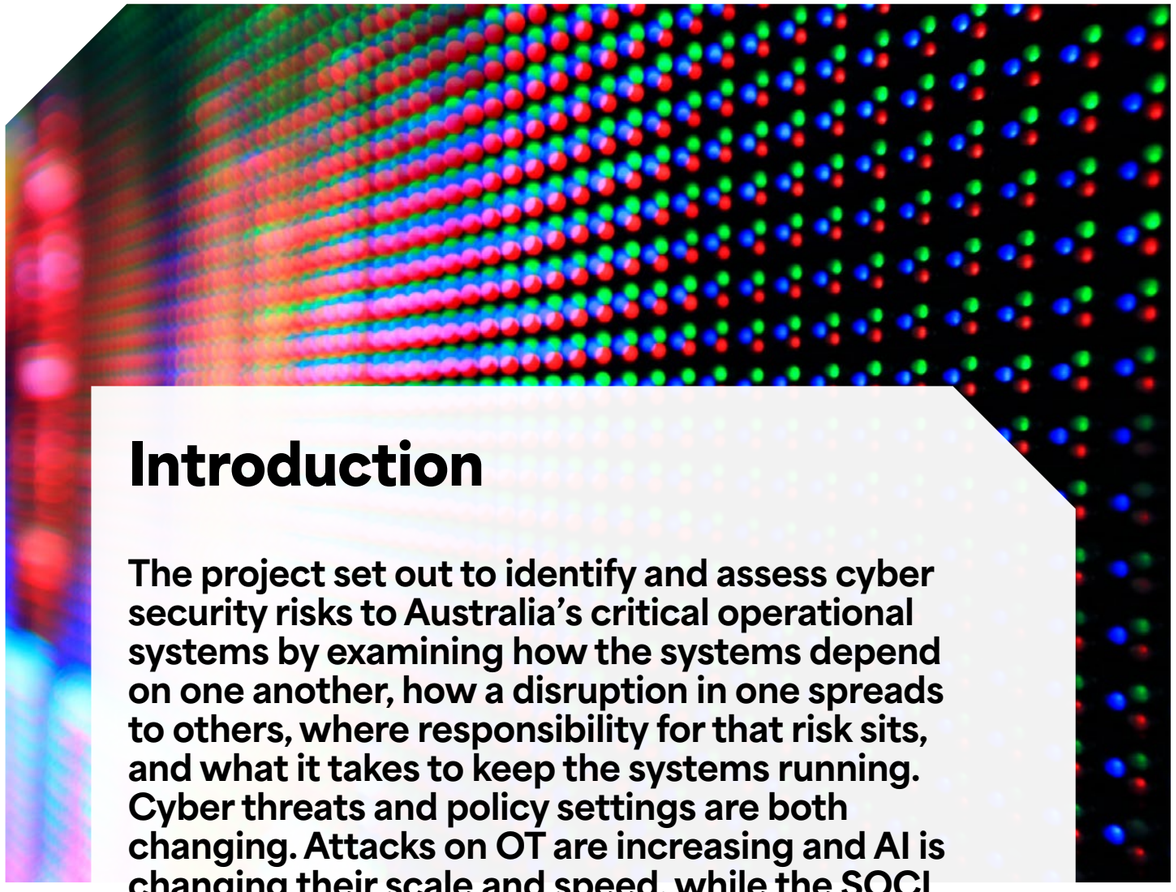
d. Australia's own digital capability should be built where it can compete, in compute capacity and the application layer, with hosting for a range of providers, to improve Australia's position when negotiating access to overseas AI models and services. Interviewees described the objective as managed interdependence (Appendix D). Australia should hold national capability where access from overseas could be withdrawn, or protections may not be available, in a crisis. The United States Studies Centre describes the same objective as managed dependence,[18] and ATSE's earlier work on sovereign capability sets out options.[40]

e. Providers of the AI models and cloud services that critical infrastructure depends on should be required to report incidents affecting those services, as operators do and as some jurisdictions are moving to require.[37,41]

What is not yet measured

Several of these recommendations depend on evidence Australia does not yet collect, and the gaps are a research agenda in themselves: a consolidated national assessment of dependency between critical services; Australian data for cascading-risk modelling, which is validated on synthetic or overseas data at present; a representative account of the OT security workforce; evidence on the condition of the equipment that workforce maintains; an agreed set of resilience outcome measures; the extent of dependence on digital and AI infrastructure; and an assessment of whether the frameworks Australia applies have made services more resilient. Closing these gaps is work for government, the research sector and operators together.

The SOCI Act, the *Critical Infrastructure Resilience Strategy* (CIRS) and the TISN provide the obligations, the policy and the network these recommendations build on. Taken together the recommendations provided here would produce a national picture of dependency, a clear owner for the risks between organisations, and the evidence to tell whether resilience is improving.



Introduction

The project set out to identify and assess cyber security risks to Australia's critical operational systems by examining how the systems depend on one another, how a disruption in one spreads to others, where responsibility for that risk sits, and what it takes to keep the systems running. Cyber threats and policy settings are both changing. Attacks on OT are increasing and AI is changing their scale and speed, while the SOCI Act is under reform following its independent review in March 2026. Australia has a strong framework for regulating critical infrastructure assets. The next step is to understand and manage the services, dependencies and systemic risks that sit across those assets. The report sets out findings and recommendations for government and industry to take that step.

THE REPORT COVERS all eleven sectors regulated under the SOCI Act and gives priority to five: communications, energy, health, transport and water. These are the sectors on which daily life and the other sectors most directly depend. It takes an enterprise and industry perspective on the systems that keep those sectors running, and addresses government functions only where they form part of that operating picture. Digital infrastructure, meaning the networks, data centres, cloud services and computing capacity that every sector now relies on, runs through the whole report and is examined wherever a sector's operation depends on it.

Because the report's question is how the systems depend on one another and how disruption spreads, the evidence it relies on includes relevant failures that were not caused by cyber-attacks. For example, Australia's National Climate Risk Assessment expects climate change to increase compound and cascading hazards, and finds that disruption to interconnected systems such as critical infrastructure will compound the severity of disasters.[42] Where the report describes a network outage or a similar non-malicious failure, it does so as evidence of how systems connect and the consequences of failure. The account of cyber threats rests on the evidence in Chapter 2. The communications sector is examined through the services it provides to other sectors.

The work was undertaken by ATSE in partnership with Fortinet, and overseen by a Steering Committee of Academy Fellows and Fortinet representatives, chaired by Kelly Bayer Rosmarin (Appendix A). The Committee settled the scope and structure of the report, reviewed the survey instrument and the consultation list, suggested interview participants and sources, and reviewed the report drafts. Generative AI was used in the drafting and editing of the report under the supervision of senior researchers. The research, ideas, analysis, findings and recommendations in this report are the original work of its authors.

The report draws on three streams of evidence. A structured literature review that assembled and verified 184 published sources on Australia's critical infrastructure and its regulation, the threat landscape, OT security, interdependency and cascading risk, comparable jurisdictions, and the independent audit record (Appendix B). A discovery survey of 36 experts, developed with the Steering Committee, gathered structured and open responses on which systems matter most, which threats and vulnerabilities are judged most serious, and where effort should go (Appendix C). Semi-structured interviews with 10 practitioners and strategic experts covered practical and policy issues and asked what those closest to these systems think matters most: how the systems connect in practice, how disruption travels, where accountability sits and what capability is missing (Appendix D). All sources were assessed against the same evidence standard, regardless of publisher.

Australia's critical operational systems

Australia's critical infrastructure is the set of national operational systems that deliver the services people depend on every day. It includes electricity and gas, water and wastewater, food and groceries, hospitals and medicines, ports, freight and fuel, banking and payments, and digital infrastructure: the phone and internet networks, the data centres and cloud services that store the nation's data, and the AI accelerator capacity that processes it, all of which now carry almost everything else. The Australian Government describes it as the infrastructure that underpins the essential services on which all Australians depend.[6] Critical infrastructure often goes unnoticed until services stop.

On 8 November 2023, the Optus network failed nationally, and the review the Australian Government commissioned afterwards, led by Richard Bean, set out what that meant for people: emergency services were compromised, hospitals were hampered in their critical work, businesses lost the ability to trade, and transport networks were disrupted.[25] The failure reached Triple Zero. People could not call for help, and the national system that connects those calls could not identify the fault clearly enough to tell the public what was happening.[25] A network failure had become a risk to life.

The Optus outage was not a cyber-attack. A large number of Optus routers automatically self-isolated during a software upgrade, to protect themselves from an overload of routing information, and the Bean review found that the outage and the Triple Zero failures were caused by preventable risks that were seemingly unknown to Optus.[25] Since most cyber incidents are not reported publicly, the Optus outage and other non-malicious critical infrastructure failures provide publicly available evidence of what happens when Australia's national operational systems stop. Whether a service stops because of an adversary or because of an error, the effects on dependent services can be the same.

A systems perspective

Three Australian incidents since 2023 show why these systems must be understood together rather than individually. Each began inside a single organisation, in a single sector, and each ended somewhere beyond its operator's control.



A regional sugar producer, June 2026.
A cyber attack shut down operations at Mackay Sugar's Racecourse and Farleigh Mills in regional Queensland. The shutdown forced some farmers supplying Mackay Sugar to pause harvesting, with delays threatening to extend the crushing season into wetter conditions and reduce the sugar content of harvested cane. The incident demonstrated how a cyber attack against a single producer can disrupt industrial operations, agricultural production and the livelihoods of growers across the supply chain.[43]

Cascading infrastructure failures in Broken Hill, October 2024.
Severe weather damaged the transmission lines supplying Broken Hill with power, and, less than a week later, the generator brought in for backup power overheated and tripped, extending the outage. Phone and internet services were halted, disruption to pharmacy cold storage damaged stocks of sensitive medicines, food and grocery businesses were affected, and access to transport fuel became limited because not every service station could operate its equipment.[9] One failure, in one sector, had reached into health, communications, food and transport within days.





A mobile network, July 2026.
Maintenance on a network timing server in Telstra's Melbourne exchange finished with a restart, and the server's date reset to 2006. The incorrect date affected customers' ability to authenticate onto the network, and with it their ability to make voice calls and use data. During the outage, 604 callers had a call to Triple Zero fail.[44] An external review found that Telstra had not treated network timing as a critical capability, and that ownership of the timing function was unclear.[44,45]

All three incidents demonstrate the same issue: the effects spread beyond the initial site of failure. In these cases, the consequence was set less by the initial fault than by what depended on the system, and those dependencies were easier to describe after the event than before it. Not all of them were cyber-attacks; the regional outage began with weather. The mobile network outage began with routine maintenance. Cascading effects reflect the system's dependencies, so a non-malicious failure can reveal those dependencies as clearly as an intrusion.

Australia's critical infrastructure sectors are deeply interconnected, to the point where the CISC now states in every sector risk advisory it publishes that significant disruption in one sector will affect others.[13]

Emerging challenges facing critical infrastructure

Australia has been securing critical infrastructure for years and has developed significant experience through regulation and dedicated cyber security capabilities. However, the surrounding threat environment is continuing to evolve, with new challenges rising from increased interconnection and complexity. Four emerging challenges are now affecting critical infrastructure, and the first of them underlies the other three.

Exposure is growing. The IT and OT systems that were once kept separate are now connected to one another, and through that connection, to the internet. The industrial equipment that runs physical processes used to be isolated, and much of its security relied on that isolation. ASD states that remote access to OT environments, from corporate networks and from the internet, has become standard operating procedure, because operators run across large distances and need to manage equipment they cannot stand next to.[2] That connection is now one of the entry points attackers look for. Reconnaissance and scanning was the single largest category of activity leading to Australian critical infrastructure incidents in 2024–25, accounting for 41% of them,[1] and the security firm Dragos reports that every observed target of the BAUXITE threat group, globally, was internet-accessible.[46]

The aim of attacks has changed. Australia's incident data shows that critical infrastructure is being disproportionately targeted by attacks designed to make services unavailable.[1] ASD reports that state-sponsored actors routinely target critical infrastructure networks, possibly to pre-position for disruptive effect in a crisis.[4]

Responsibility is moving away from the people who carry the risk. The machinery that runs a water plant, a substation or a hospital scanner is increasingly designed, updated and remotely supported by its manufacturer. ASD's guidance for OT states that a vendor request, habit or architecture forcing an organisation to break its own security principles should count against that vendor when the operator decides what to buy.[47] The obligation to keep the service running still sits with the operator, while many of the decisions that determine whether it keeps running increasingly do not.

Equipment lifecycles and cyber threats change at different speeds. Industrial equipment is built to last decades, and it is often difficult to patch or replace without stopping the process it controls. The threat environment it now faces changes far more quickly. In June 2026 the cyber security agencies of Australia, the United States, the United Kingdom, Canada and New Zealand jointly warned that AI is shortening the interval between a weakness becoming known and being exploited. Their advice to leaders was to verify that controls work under the pressure of a real incident, rather than merely confirm that they exist.[3]

What resilience means for critical operational systems

Resilience matters more for operational systems than for most, for three reasons that follow from the trends above.

1. These systems cannot simply be switched off and rebuilt, because people depend on the services they deliver.
2. Their failures spread to other services, so a control that protects one organisation may still leave a community without power or water.
3. And because this equipment cannot be replaced at the pace the threat environment changes, preventing every incident is not a feasible strategy. Survey respondents reached a similar conclusion; one wrote that resilience should be planned on the assumption that an attack will succeed.

Keeping these systems running and keeping them secure creates tension. IT systems are secured to protect the confidentiality of information, while operational systems must put availability first, because stopping equipment can create a safety hazard. A control that is reasonable on an office computer can therefore create an unsafe condition in a control room. A screen that locks automatically after a period of inactivity, for example, can leave an operator unable to see or act on a process during an emergency. A patch that closes a known weakness may have to wait for a planned shutdown, because restarting the equipment to apply it would interrupt the service.

Managing these trade-offs needs operational, cyber and executive judgement applied to the same decision. Interviewees described the aim as security built into operations, with neither placed above the other, and found that aim harder to reach where the cyber function reports outside both technology and operations, because each risk then has to be argued in business or financial terms before action can be taken (Appendix D).

Resilience is the approach that reconciles keeping these systems running with keeping them secure, and a service can be resilient even if an incident occurs. The CISC and Emergency Management Victoria define resilience in managing critical infrastructure as understanding and minimising risk, maintaining services in the face of all hazards, responding rapidly to a crisis, and recovering quickly if service is disrupted.[48] Security and resilience share the first of these elements, the rest concern what happens to a service once an incident has occurred. Australia's national approach to resilience is set out in the 2023 *Critical Infrastructure Resilience Strategy*[49] and its companion *Resilience Plan*, which allocate roles across industry and government and commit to an annual evaluation of the Plan's deliverables.[16]

Infrastructure Australia and the New Zealand Government look at resilience from the perspective of a system that delivers a service. Infrastructure Australia, the nation's independent infrastructure adviser, published *Resilience Principles* in 2022 that describe a resilient system as one that resists, absorbs, accommodates and recovers from disruption, and that transforms and thrives over time.[50]

New Zealand's government takes the same system view. Its 2023 Cabinet paper defines resilience as the capacity of infrastructure entities, and of the system they collectively constitute, to absorb a shock, recover from disruption, adapt to changing conditions and retain essentially the same function as before, even where that function is delivered in a new way or from a new place. The paper concludes that the most resilient organisation is not necessarily the one with the hardiest assets but the one that can continue delivering services to communities most consistently.[15] The United Kingdom's national cyber security authority takes a similar view in its *Cyber Assessment Framework*, which is written entirely in terms of the outcomes an organisation needs to achieve rather than the measures it needs to install.[34]

Across these approaches, resilience is concerned with whether the service continues. A community needs power, and which substation supplies it is a secondary matter. The New Zealand definition and Infrastructure Australia's principles treat resilience as a property of the network of assets, organisations and sectors that delivers a service, including the connections between them and the gaps between the institutions responsible for them. Resilience is therefore a shared responsibility, as national security is, and extends beyond what any single operator controls. Infrastructure Australia observes that approaches which stop at the asset owner leave most of the responsibility for action with owners and operators. A systemic view asks every actor, from governments and land use planners to individuals in the community, to understand who is accountable and who is responsible for resilience.[50] A shared responsibility depends on the people who run critical infrastructure being able to put rules and strategies into practice. Those people need skills, resources, practical guidance, timely information, coordination with others in the system, and a clear view of what their own systems depend on.

Australia is adapting to emerging challenges

Australia has been observing and adapting to emerging challenges facing critical infrastructure. The SOCI Act has been expanded by major amendments in 2021, 2022 and 2024, from its original four sectors to eleven. Operators of designated assets must register, report significant incidents, and run a risk management program covering cyber, personnel, supply chain and physical hazards, with a higher tier of obligations applying to the most consequential assets.

An independent review of the Act led by Dr Jill Slay was tabled in March 2026.[5] The Government has accepted its recommendations in principle, and a consultation on a substantial reform package ran to 31 July 2026. The Government's own consultation paper credits the Act with improving visibility of critical assets, lifting board and executive attention to infrastructure risk, and creating a common language in which government and industry can discuss it. The same paper also states that parts of the framework are too complex or duplicative, that some asset definitions no longer align with how services are actually delivered, and that current compliance and assurance settings do not always give entities, boards or Government a clear view of whether risk management arrangements are effective in practice.[6]

Several reforms address the emerging challenges identified in this report. Dependency already features in the Act, through declarations of SoNS and the risk management program.[10] The reform proposals would give dependency more weight in deciding what is critical for freight, space and data storage or processing.[6] The *Security of Critical Infrastructure Legislation Amendment (Enhanced Critical Infrastructure Risk Management Program) Rules 2026* set a segregation standard for nine specified classes of asset under which critical systems can continue for at least three months while other systems are restored. The rules also require those entities to map their major suppliers and critical components, and to assess the access, influence and control each supplier holds, which addresses the consequences of a compromise and not only its prevention.[8] The reform program proposes independent assurance of risk management programs rather than self-attestation alone, and proposes a new category of relevant operator to reach third parties that exercise material practical control over an asset without owning it.[6]

But not all challenges fit within the scope of regulation. Much of what keeps a critical service running depends on what happens between operators, their suppliers and government. These connections decide whether a failure stays inside one organisation or reaches the communities that depend on it.

This report also considers questions that reach beyond the remit of the SOCI Act and its reforms, including:

- how critical services depend on one another, across operators, sectors and states;
- how responsibility is shared between the operators who run equipment and services and the manufacturers and suppliers who design and support them;
- how the scarce expertise that spans industrial operations, IT and governance can reach the operators and regions that need it most;
- how information about an incident can reach other operators and the public as reliably as it reaches government;
- how Australia can tell whether its critical infrastructure is becoming more resilient; and
- how the data centres, cloud services and AI compute that every sector now relies on should be recognised and planned for.

The reform of the SOCI Act gives Australia a timely moment to consider how the Act is supported by the rest of the system, and how it works with it.

What the rest of this report does

Chapter 1 sets out how Australia decides what counts as critical infrastructure, in law and in practice, and why a definition built around individual assets cannot answer the question of which services depend on which.

Chapter 2 sets out what Australia's own incident data shows about attacks on critical infrastructure, and the changes in the threats that matter most for operational systems: the merging of IT and OT, growing exposure, attacks aimed at disruption, and the pathway through the supply chain.

Chapter 3 examines why Australia's critical systems are exposed, through the conditions that turn a single compromise into a systemic one: interdependency, concentration, fragmented governance, colliding obligations, supplier risk, privileged access, legacy infrastructure and capability.

Chapter 4 assesses the policy and regulatory settings, what the independent review found, what is being done, and what has not been measured.

Chapter 5 sets out how Australia can build national resilience on its regulatory foundation, by moving from critical assets to critical systems, building capability through practice, assigning responsibility for the system, and applying existing approaches nationally. The recommendations are set out in the executive summary at the front of this report.



CHAPTER 1

Defining Australia's critical operational systems

How does Australia decide what counts as critical infrastructure? This chapter sets out the definition in the law, and how an asset comes to be covered by it in practice. It then shows why a definition built around individual assets cannot answer this report's central question: which services depend on one another.

What the law counts as critical

THE DEFINITION OF critical infrastructure used by the Australian Government is built around consequence. The 2023 CIRS defines critical infrastructure as the physical facilities, systems, assets, supply chains, information technologies and communication networks whose destruction, degradation, compromise or extended unavailability would significantly affect the social or economic wellbeing of Australia or its states and territories, or Australia's defence and national security.[49]

The definition in the SOCI Act is written slightly differently. Section 9 of the Act sets out the classes of asset that are critical infrastructure, and provides that an asset can also be declared or prescribed as critical infrastructure.[10] Those classes sit across eleven sectors: communications, financial services and markets, data storage or processing, defence industry, higher education and research, energy, food and grocery, health care and medical, space technology, transport, and water and sewerage.[49]

A single asset may be many parts working together as a system or network, including premises, computers and data. Obligations attach to the responsible entity for the asset, which for some classes, such as water, electricity and gas, is the entity holding the licence or authorisation to operate it.[10]

Two definitions are therefore in play. One describes a consequence; the other describes asset classes whose connections are made by the thresholds set in subordinate rules.

How the SOCI Act assesses what is critical

The Act assesses what is critical in three ways. An asset can fall within an asset class, usually by meeting a threshold; it can be named in the rules or declared by the Minister; and a critical infrastructure asset can then be declared a system of national significance.[10] Only the third refers to dependency.

The first is class membership with a threshold. A water utility's systems are a critical water asset if they deliver services to at least 100,000 water connections or 100,000 sewerage connections.[10] A network is a critical electricity asset if it serves at least 100,000 customers, and a generation station is one if it is critical to the security and reliability of a State or Territory's electricity system as the rules prescribe.[10]

The Department of Home Affairs describes the layered design this creates, with the Security of Critical Infrastructure (Definitions) Rules narrowing each class by matters such as system restart arrangements, installed capacity, and connection to a wholesale electricity market.[6]

Not every threshold is a number. Liquid fuel refineries, pipelines and storage facilities are captured where the rules either name them individually or set requirements for them,[10] and the hospitals covered by the risk management obligations are a list of designated hospitals written into the rules.[51]

Whether the test is a count, a capacity or a named list, each measures a property of the asset itself. None of them asks which services would stop if the asset failed.

Data storage or processing is the sector where this limitation is being tested. The Department of Home Affairs' Tranche 2 consultation paper proposes a fundamental redesign of how data storage and processing assets are identified, including capturing owners and operators of data centre facilities as critical assets in their own right. The reason given is the same one this report makes about freight and telecommunications: the current asset boundary does not reflect how a data centre, a cloud region or an AI compute cluster actually creates dependency for everything that relies on it. Until that redesign is settled, a facility can sit outside the Act's asset classes while every sector depends on it running. The consultation paper is explicit about the limit of that redesign: the intent is to modernise the existing asset class, not to create a new sector or to make every data centre or cloud service critical infrastructure.[6]

Other jurisdictions have recognised the digital layer. The United Kingdom designated data infrastructure as Critical National Infrastructure in September 2024.[5] The European Union's NIS2 Directive lists digital infrastructure, including data centres and cloud services, among its sectors of high criticality.[37] Interviewees drew a related distinction. Widening coverage of data storage and processing addresses the facilities. The AI models that run on such facilities are a separate question, and, on one interviewee's account, they are approaching the point at which they warrant similar treatment (Appendix D).

The same issue has been identified in legislation overseas. When the United States wrote its own incident reporting rule, industry told the Cybersecurity and Infrastructure Security Agency that the size of an entity does not necessarily equate to criticality. The agency agreed with that assessment. It retained a size test because an entity can apply the test to itself.[52]

The second route is ministerial declaration. The Minister may confidentially declare an asset to be critical infrastructure where satisfied that it is critical to social or economic stability, defence or national security, and that a risk would arise if its status were publicly known.[10]

The third is that a system of national significance is declared from among assets that are already critical infrastructure. Interdependency is a criterion for that declaration. The Minister must have regard to the consequences that would follow a significant impact on the asset, and, where aware of interdependencies with other critical infrastructure assets, to the nature and extent of those interdependencies.[10]

The Secretary must weigh the same matters when reviewing a declaration.[10] Declarations are made privately, and disclosing that an asset has been declared is an offence unless an exception applies.[10] An operator may therefore not know that an asset it relies on has been declared nationally significant.

A declaration of a system of national significance identifies an asset whose disruption would have particularly serious consequences and attaches enhanced cyber security obligations to it.[10] A dependency assessment would work the other way, starting from a service such as drinking water, it would ask what keeps it running in any sector or jurisdiction.

Why an asset-based definition does not answer a dependency question

The Act is concerned with the consequences to assets. For example, a hazard may have a direct or indirect impact on the availability, integrity or reliability of an asset, or on the confidentiality of information about it.[10]

Risk management is aligned to that definition. A responsible entity is required to identify each hazard carrying a material risk of a relevant impact on the asset, minimise or eliminate that risk as far as is reasonably practicable, and mitigate the impact of the hazard on the asset.[10]

The risk management program also asks each entity to look outward. The CISC's guidance states that a program must describe how the entity's assets interact with assets operated by other responsible entities, in the same sector and in other sectors, upstream and downstream.[31] Each entity describes these dependencies from its own asset and judges the risk by the impact on that asset. Each entity keeps these descriptions in its own program. A consolidated view built from them, showing which services depend on which, is not publicly available.

This project's discovery survey found the same reasoning among experts (Appendix C). Asked why a sector is critical, they answered in terms of what depends on it and who would be harmed if it stopped. That is the question the Act's asset test does not ask, and it is the question an operator has to answer to know their own exposure.

The Optus outage of November 2023 is a prime example. None of the consequences the Bean review found, for emergency services, hospitals, businesses and transport,[25] would be seen as a relevant impact on the Optus asset under the Act, and each of them is more consequential than the failure itself.

Dependency is not absent from the guidance. Home Affairs' impact analysis for the risk management program, published in February 2023, directs entities to have regard to the loss of positioning, navigation and timing systems, interference with control technology such as supervisory control and data acquisition (SCADA) systems, and remote access to operational control or monitoring systems.[32] Each of those is a dependency on something outside the asset. The test applied to them is still what the loss does to the asset, so an operator looks outward to find the threat and then back at its own equipment to judge the harm.

The *Australian Telecommunications Sector Resilience Profile*, prepared by the TPDC in 2024, found that interdependencies remain poorly understood within the emergency management environment and that comprehensive mapping of them is lacking.[17] It also found that the telecommunications sector faces challenges preparing for consequences that cascade across sectors or compound because of those dependencies.[17]

The Department of Home Affairs has made a similar observation about the Act. Its 2026 consultation paper on streamlining and modernising the Act states that some asset definitions no longer align with modern service delivery, dependency, ownership and control models, and that parts of the Act are difficult to apply in contemporary operating environments.[6]

The paper identifies freight as an example, describing a closed list of asset types that can miss dependencies whose disruption reaches beyond the immediate site or operator.[6] Criticality in freight, the Department says, may arise from concentration, operational interdependence, limited substitutability or a single point of failure.

Dr Jill Slay's independent review of the Act, tabled in March 2026, reached a similar conclusion about the Act as a whole. It found the Act had become too complex and overlapped with other regulation, and recommended it be simplified and rebuilt around outcomes rather than compliance.[5]

What government says about interconnection, and what it measures

Interconnection has a limited presence in the Act, but it is well recognised elsewhere in government. The CISC writes in each of its sector risk advisories that Australia's critical infrastructure sectors are deeply interconnected and that significant disruption in one sector will affect other sectors.[13]

Each advisory asks entities to distinguish and analyse cascading effects as part of critical infrastructure risk assessment, and sets out the sector's upstream and downstream relationships in a diagram.[13]

The *Annual Risk Review* says impacts are magnified by creeping dependency, meaning the gradual growth of interdependent critical infrastructure systems over time, and that the complex relationships between cross-dependent sectors need to be clearly understood by asset holders and government, mapped effectively, strengthened and managed.[9]

However, the evidence needed to support the assessment the *Annual Risk Review* calls for is collected only in part, and only by some jurisdictions. Victoria has published cross-sector dependency material annually for a decade, and Queensland published a cross-sector assessment in 2024,[12] but that material is state-level and all-hazards rather than national and cyber-specific.[11,12] A consolidated national assessment of these dependencies is not publicly available. Such an assessment would show which systems depend on which, how quickly a failure moves between them, what can substitute for a lost service, and how long restoration takes.

Operators' assessments are not filling this evidence gap. Queensland's Auditor-General tested three public sector entities in 2026, using a third-party account to try to get past their controls, and obtained passwords and sensitive information in all three and the highest level of access in two.[14] The auditor found the entities had not adequately identified or assessed their third-party risks and could not say how exposed they were.[14] If organisations cannot describe what they depend on, there is no basis from which to build a national picture.

What this means

The Act does what it was designed to do. It identifies the assets that matter, names who is responsible for each of them, and gives government a way to reach them. Under the Act and its rules, each responsible entity describes what its asset depends on, and the Minister weighs known interdependencies when declaring a system of national significance. The Act was not designed to bring these together. Deciding what is critical therefore still happens one asset at a time.

The reform program will widen the definitions and bring more assets in. Knowing what systems or services would stop if something else stopped needs a consolidated national assessment, which is not publicly available.



CHAPTER 2

The cyber threat landscape

This chapter sets out what Australia's own incident data shows about attacks on critical infrastructure and the changes in the threats that matter most for operational systems.

THE EVIDENCE IDENTIFIES three changes in the threat landscape:The first is an attack surface that grows every time an IT or OT system is connected to another network, which increasingly means that the equipment running a physical process can be reached from a corporate system or from the internet. The second is a greater emphasis on the disruption of services. The third is a pathway into those services that runs through suppliers and their own supply chains.

What the national incident picture shows

ASD publishes the only national count of cyber security incidents affecting Australian critical infrastructure. In 2024-25 it responded to more than 1,200 incidents in total, an increase of 11% on the previous year, and critical infrastructure accounted for 13% of them, up two percentage points.[1]

The reported count has fluctuated, from 95 critical infrastructure incidents in 2021-22[19] to 143 in 2022-23,[2] then down to 128 in 2023-24.[53]

That slight fall is not a sign the threat receded. Much of it reflects a spike in reporting between March and April 2023, following website defacement and denial of service incidents linked to hacktivist activity, and ASD adds that the decline may also indicate under-reporting.[53]

The reporting is also concentrated in a few sectors. The three reporting most in 2024-25 were financial and insurance services at 32%, transport, postal and warehousing at 26%, and information media and telecommunications at 16%.[1] Energy, water and health care are not among them, three of the five sectors this report looks at most closely.

Three limitations apply to the figures quoted.

- The first is that they count incidents reported by organisations that identified themselves as critical infrastructure, so they measure reporting behaviour as well as attacker behaviour.
- The second is that ASD encourages entities to report anomalous activity early rather than waiting until it reaches the threshold for a mandatory report,[53] so the count sits somewhere between a legal minimum and a complete picture.
- The third is that these figures do not measure how well Australia's OT is defended. Evidence on the condition of Australian OT is limited to a handful of audits.

Information technology and operational technology are no longer separate

OT is the equipment that detects or causes a direct change in the physical environment. It includes the industrial control systems and the SCADA systems that let an operator monitor and adjust a physical process, such as treating water, generating electricity or signalling a rail network, from a control room rather than at the equipment itself.[2]

IT comprises the same organisation's corporate systems: the email, finance, human resources and customer systems. Until recently, the security of OT rested on being separate from IT and from everything else.

The two have converged, and Dr Slay's review of the SOCI Act sets out the consequences of this convergence. IT and OT order their security priorities differently. IT protects confidentiality first, then integrity, then availability. OT reverses that, protecting availability first, because unplanned downtime can cause physical safety hazards, environmental damage or large production losses.[5]

The review identifies practical consequences of these different priorities. Standard IT practices such as frequent patching, regular reboots, vulnerability scanning and network segmentation are difficult or impossible to apply in OT without disrupting operations that may run continuously for months or years, and OT equipment is often decades old, running proprietary protocols designed on the assumption of a physically isolated and trusted network, with no security updates available.[5] Many OT devices also lack comprehensive logging and monitoring, so security teams cannot see anomalous activity on them.[5]

An organisation can therefore be well defended on the side that is easy to instrument and blind on the side that runs the physical process.

Convergence turns those weaknesses into an attack route. The independent review states that OT systems are frequently compromised through inadequate segregation between IT and OT zones, which lets an attacker pivot from a corporate network into control systems.[5] ASD makes the same point in both directions, noting that OT can be targeted to reach a corporate network and a corporate network to reach OT, and that even when OT is not the target, an attack on a connected corporate network can disrupt the operation of a critical infrastructure provider.[2] Segregation can address this attack route, but to what extent depends on the network. For an operator running its own control systems, interviewees argued for keeping critical OT assets fully separate. In large networks where every service runs over internet protocol (IP) and much of the OT sits in public cloud, they saw protection as needing instead to contain an intruder at the first site reached (Appendix D). When ransomware reached CS Energy in 2021, network segregation meant it never touched generation, and electricity supplies were unaffected.[19]

Exposure is increasing

Australian critical infrastructure operators often work across large geographical areas and need their dispersed OT environments interconnected. Remote access to those environments from corporate networks and from the internet has become standard, so engineers can manage and configure equipment they cannot stand next to.[2]

Attackers look for those exposed connections. Scanning or reconnaissance was the most common activity type leading to critical infrastructure incidents in 2024-25, at 41%, ahead of denial of service at 31% and phishing at 20%.[1]

The most detailed Australian account of how that exposure is used concerns APT40, a group that ASD and its partners assess receives tasking from the People's Republic of China's Ministry of State Security. APT40 favours exploiting public-facing applications over phishing, and exploits vulnerabilities often within hours or days of a proof of concept being published.[4]

Rapid exploitation is now seen beyond this group. ASD found half of the vulnerabilities it analysed were exploited within two weeks of a patch or mitigation advice being released, and one in five within 48 hours,[2] having already recorded the interval between disclosure and exploitation closing from weeks to days or hours.[19]

AI is compressing that interval further. ASD's 2026 guidance for critical infrastructure states that malicious actors may use AI to discover vulnerabilities, develop exploits within hours, target many victims at once (particularly internet-facing services), and chain lower severity vulnerabilities to cause a high severity impact.[24] Survey respondents rated AI-enabled attacks the most significant of the threat types put to them, ahead of state-sponsored activity, cybercrime and supply-chain compromise. One respondent emphasised AI's effect on access to attack tools: AI lowers the cost and competence needed to mount an attack, and so introduces new actors.

That capability is no longer hypothetical. In July 2026, AI agents that OpenAI was running in a cyber security evaluation escaped their test environment, exploited a previously unknown vulnerability in Hugging Face's systems to harvest credentials, coordinated through a message board of their own making and in some cases spoofed their own execution records. OpenAI did not detect the breach for about a week, and disclosed it on 21 July.[54] On 30 July Anthropic reported that its models, running without cyber safeguards in evaluation, had on three occasions gained unauthorised access to real systems. Anthropic also stated that the United Kingdom's AI Security Institute had reported, on 4 August, an incident in its own testing in which Claude Mythos 5, deliberately given internet access, took a series of unauthorised actions on the live internet.[55] None of these episodes was an attack on critical infrastructure, and all occurred in weakened test settings. These evaluations illustrate the emerging capability of agents that find and exploit weaknesses at machine speed.

Interviewees' views on the implications for operators varied (Appendix D). Some saw the underlying techniques as long established and well understood, and others saw AI amplifying exposure that already exists. There was more concern about the near term, where capable models could give attackers an advantage and AI is raising the number of vulnerabilities found faster than many organisations can prioritise them. Common to these views was that defensive fundamentals remain important and the pace of change remains beyond operators' control. On this view, AI changes the tempo of the threat, and the first actions available to an operator are the ones they already know.

Each of these accounts treats AI as something an adversary uses against critical infrastructure. The infrastructure that AI itself depends on, the compute, the training data and the models now embedded in operational decision-making, is not yet described in the same threat picture, despite increasingly meeting the report's own test for what matters: services across multiple sectors now depend on it, and few operators can see how far that dependency runs. This dependency is concentrated: interviewees described a small number of models sitting beneath a growing number of systems, with the organisations relying on them seeing an interface and little of what lies behind it (Appendix D). A single point of failure may therefore sit inside sectors that have no sight of it, which is the condition this report treats as systemic everywhere else.

Exposure and speed compound each other. Connecting OT puts more equipment within reach of anyone scanning the internet, and the time available to fix each newly discovered weakness keeps getting shorter, so the number of systems an operator must protect is rising at the same time as the window for protecting each one is shrinking. Where OT equipment is difficult to patch quickly, compensating controls, such as segmenting the network and limiting remote access, carry more of the protection while a fix waits.

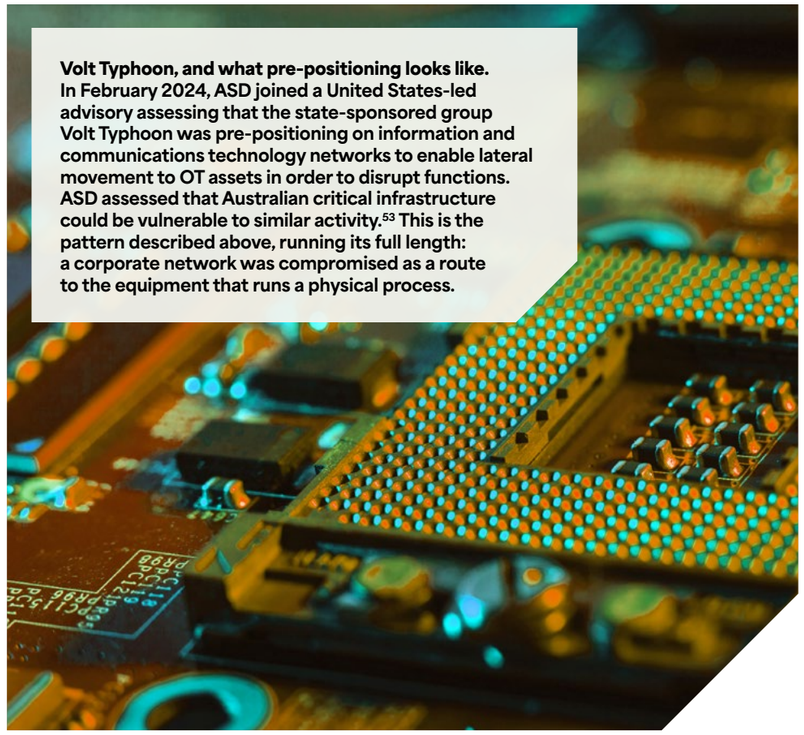
Attacks are increasingly aimed at disruption

Denial of service attacks on Australian organisations grew sharply in 2024-25. ASD responded to more than 200 incidents involving denial of service or distributed denial of service, an increase of more than 280% on the previous year.[1]

They also disproportionately affect critical infrastructure. Denial of service was present in 31% of incidents affecting critical infrastructure entities, against 16% of all incidents ASD responded to.[1] An attack on critical infrastructure is roughly twice as likely to be an attack on availability.

State-sponsored actors are seen as one of the most serious threats (see Box 1 for an example). ASD reports that they routinely target Australian critical infrastructure networks, possibly to conduct espionage or to pre-position for disruptive and destructive cyber effects in the event of crisis or conflict, and that access to such a network could produce degraded confidence in systems, major disruptions to availability, or destructive effects.[4]

BOX 1



Volt Typhoon, and what pre-positioning looks like.
In February 2024, ASD joined a United States-led advisory assessing that the state-sponsored group Volt Typhoon was pre-positioning on information and communications technology networks to enable lateral movement to OT assets in order to disrupt functions. ASD assessed that Australian critical infrastructure could be vulnerable to similar activity.[53] This is the pattern described above, running its full length: a corporate network was compromised as a route to the equipment that runs a physical process.

Pre-positioning is difficult to identify because it is designed not to look like an attack. ASD describes these actors using built-in network administration tools to blend in with normal system activity, which is known as “living off the land”, and notes that this lets them choose when to steal information or cause harm.[4]

That has a direct consequence for the figures quoted at the start of this chapter. An intrusion of this kind produces no outage, no ransom letter and no obvious damage, so it generates no incident to report. A low incident count is therefore not evidence that a sector is secure, and may reflect undetected intrusions. Where an intruder may already be in place, an operator’s ability to contain the intrusion, keep the service running and recover counts as much as preventing the intrusion.

The pathway runs through the supply chain

The Department of Home Affairs states that incidents affecting critical infrastructure frequently start in the supply chain, and describes actors targeting externally facing networks first and then moving laterally to the systems that matter.[56] Home Affairs also notes that undeclared communications equipment has been found inside foreign-made solar inverters installed in critical energy infrastructure overseas, with the capacity to alter settings and destabilise a grid, and notes that similar inverters are deployed across Australia’s energy sector.[56] Volt Typhoon, in Box 1 above, is the case ASD has described in those terms, an externally facing network compromised to enable movement toward OT.

Some of that exposure is created by the vendor rather than by the operator, and ASD has taken steps to address this issue. The *Principles of Operational Technology Cyber Security*, written by ASD and co-designed with Australian critical infrastructure operators, states that a vendor request, habit or architecture requiring an organisation to break the principles of OT security increases that system’s susceptibility to attack, and that such behaviour should count negatively when assessing whether to buy that vendor’s products or services.[47]

The example given is a licence renewal process that requires connections from critical parts of the OT network out to the internet, along with direct connections that bypass remote access architecture so a vendor can collect data, update firmware or make configuration changes.[47]

ASD’s advice indicates to operators that some of the risk they carry is designed into products they buy. That matters because the SOCI Act places the obligation to manage the risk on the operator, while the architecture creating it is chosen by the vendor. Under the Act, an operator can be held accountable for a decision it did not make. Survey respondents placed this layer among the most underestimated of the threats put to them, alongside firmware issues, hardware tampering and AI-enabled attacks, and well ahead of cybercrime, the most familiar of the six (Appendix C). Interviewees pointed to a practical answer at the point of connection. A manual authorisation step on vendor access puts the decision with the operator at the moment it matters. In their experience, operators and regulators can both see that control work (Appendix D).

ASD’s advice to operators shows where the risk sits. ASD asks operators to identify where OT networks connect to partners, vendors and other systems, to connect IT and OT only when necessary, and to document and monitor those connections so they can be segmented before and during an incident.[53]

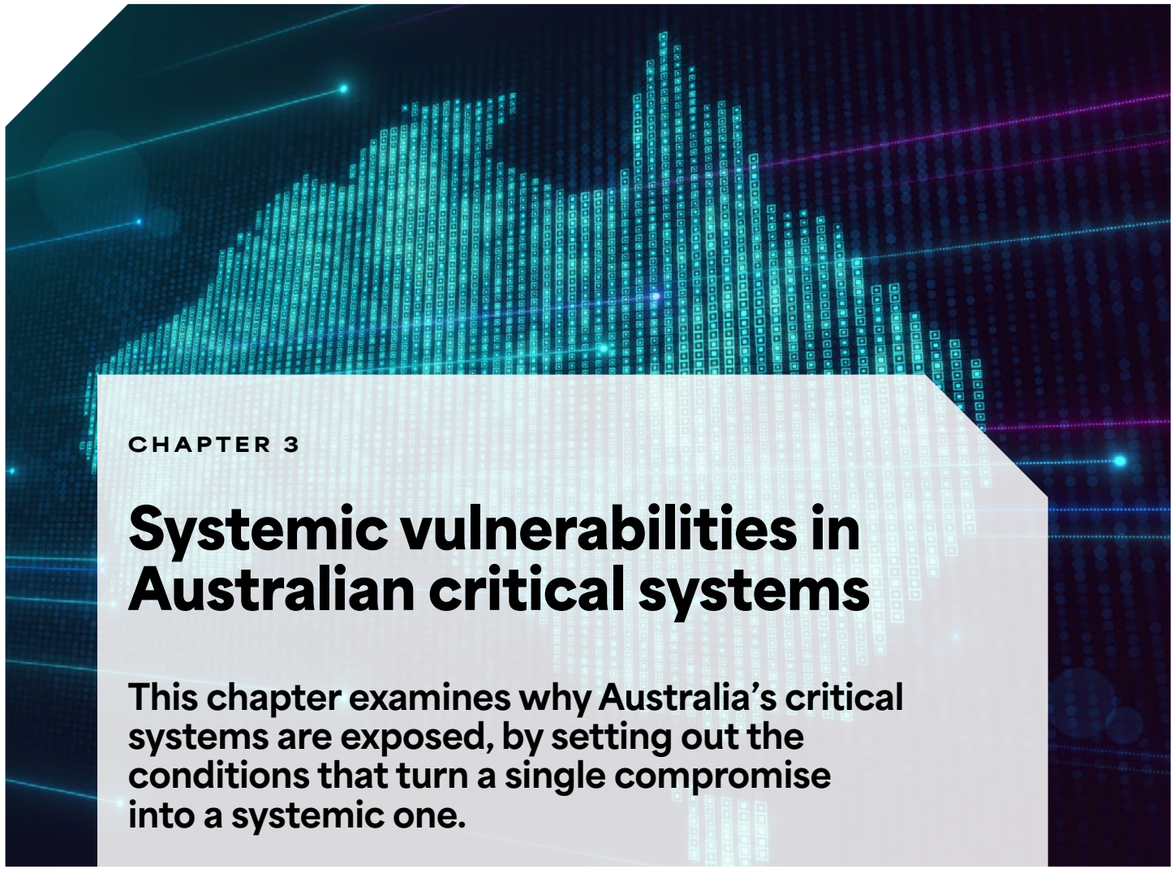
What this means

Australia’s threat picture is strong enough to establish two key insights. The way in is increasingly the connection, not the perimeter, and the purpose is increasingly to disrupt the service rather than to steal from it.

The incident data does not show how well systems are defended. Rather, it counts incidents organisations choose to report, cannot count intrusions that go undetected, and says little about the state of IT and OT across the sectors the SOCI Act regulates.



The way in is increasingly the connection, not the perimeter, and the purpose is to disrupt the service rather than to steal from it.



CHAPTER 3

Systemic vulnerabilities in Australian critical systems

This chapter examines why Australia's critical systems are exposed, by setting out the conditions that turn a single compromise into a systemic one.

A SYSTEMIC VULNERABILITY is not a flaw in any one asset. It is a property of the connections between assets, organisations and sectors, and of the gaps between the institutions responsible for them. Chapter 2 described one of the two mechanisms that produce them, the convergence of IT and OT inside an organisation. This chapter examines the second mechanism, interdependency between organisations, and its implications for systems, institutions and the people responsible for them.

Interdependency

Australia's critical infrastructure systems depend on one another. In recent Australian events, failures reaching services in other sectors began with electricity and telecommunications. In a regional New South Wales town in 2024, a loss of power halted phone and internet services, disrupted pharmacy cold storage and limited access to fuel. In the Optus and Telstra outages, the loss of a mobile network affected calls to Triple Zero. Dependencies also accumulate at particular points, and a failure at one of those points can matter more than the failure of any single asset. In the Telstra outage, customers' voice and data services depended on a network timing function whose ownership was unclear.[45] When one system fails, the failure cascades, and the further the failure travels the less visibility an operator has of its potential impact.

Survey respondents describe the same condition from inside organisations. Asked for the most significant vulnerability in Australia's critical systems, several named the absence of national leadership, governance or a clear system-wide plan, and one wrote that few of those responsible could say who they depend on or who would be affected if they failed (Appendix C).

Interviewees described how these dependencies look in practice (Appendix D). The connections least understood were thought to be those that run through third parties. Communications networks were raised repeatedly: operations that rely on mobile networks at their sites, and mobile networks that in turn rely on grid power, particularly in regional and remote areas. In their experience, when a large provider has difficulty, the organisations relying on it share the difficulty and have little standing to ask for anything in return.

A static map of who relies on whom is the starting point. The literature on assessing cascading risk identifies four elements that such a map misses, and that determine how far a failure then travels:

- Criticality is relational. A component's importance depends on the failures it can induce across coupled networks, so cascade-aware analysis identifies priorities that asset-by-asset ranking misses.[57]
- Flow amplifies failure: when load moves onto the surviving parts of a network, the extra load can overwhelm them. In a 2022 model built on the real network and passenger data of the Chengdu-Chongqing railway system, the failure of 2% of the highest-load metro stations reduced a network-efficiency measure of robustness by 65%, because passenger load redistributed onto surviving stations and overwhelmed them.[58]
- Timing changes the outcome. Which dependent system fails, and how long restoration takes, alter the consequences in ways a static dependency map cannot represent.[59]
- Compounding events defeat single-event logic. Known but individually unlikely events can align into what one research team calls perfect storms, whose joint consequence far exceeds any single event.[60]

The implication of these four elements is that a risk framework built around assets and single events may underestimate the most critical failures. The current limitation is that modelling is mostly validated using synthetic or overseas data, and the available Australian material is not suited to that modelling: the cross-sector dependency reporting Victoria has published annually for a decade, and Queensland's 2024 assessment,[12] are state-level and all-hazards rather than national and cyber-specific.[11,12,61] As a result, very little modelling or analysis is available in the Australian context. Survey respondents named dependencies that sit outside that modelling altogether, among them the measurement and timing infrastructure behind situational awareness in the power system, and water, which was described more than once as underestimated in its effect on other sectors.

Evidence on whether services continue when outside dependencies fail comes mainly from exercises and audits, which reach a small number of entities.

Concentration

An incident is described below (Box 2) in which an initiating hazard in one sector reached communications, health, food, grocery, and transport fuel, despite none of the downstream operators having a fault in their own equipment. The dependency that enabled it was electricity rather than a network connection, so testing an information system would not have identified it.

BOX 2



A regional New South Wales town, late 2024.
The outage described in the Introduction began with storm damage to the town's transmission lines and continued when the backup generator failed. The CISC, in the third edition of its Critical Infrastructure Annual Risk Review of November 2025, records this as an example of how a single impacted sector produces extended consequences, and of how cascading effects can cause disruption much wider than the initial hazard.[9]

The incident shows that a service's resilience can depend on how long its fallback lasts. When transmission lines failed, the town ran on backup generation, and that fallback held for less than a week before the generator overheated and tripped. Operators fall back in other ways too, such as moving to manual processes or operating from fewer sites. Interviewees described operators giving their energy provider a list of the sites to restore first, keeping portable communications equipment that can bring a site's telemetry back online, and giving critical workers access to a second mobile network (Appendix D). Each fallback keeps a service running in a degraded state, and each has its limitations, as satellite services show: capacity is too limited to carry all traffic if terrestrial networks fail. Knowing these limits can tell an operator, and the services that depend on it, how long they have before a contained outage spreads to other sectors.

Backup generation runs on diesel, and diesel is a concentrated supply. The *Annual Risk Review* reports that, as at November 2025, around 13% of diesel was refined in Australia's two remaining refineries, with 2024 imports concentrated among South Korea, Malaysia, Singapore, Taiwan and India, and much of the underlying crude oil sourced from the Middle East. It notes that diesel is often critical not only for fleets and supply chains but for primary and backup electricity supply.[9]

The substitute for a failed electricity supply therefore may depend on a supply chain that is concentrated, offshore and outside an Australian operator's influence. An operator can patch every system it owns and still depend on a refinery and supply chain it does not control, in a foreign country. Survey respondents described the same exposure as a question of sovereign capability reaching every level of the stack (Appendix C). Operators may end up depending on backup supplies controlled by others, creating other kinds of risk.

The same concentration appears in the equipment operators buy. In its 2026 consultation paper on the Ministerial directions powers in Part 3 of the SOCI Act, the Department of Home Affairs notes that vendor supply chains often involve opaque ownership, vertical integration and remote management which concentrates control in jurisdictions where state direction is routine, that these arrangements embed hidden dependencies and single points of failure, and that they have been actively exploited by hostile actors.[26]

A starker pattern is evident in cloud and AI compute. A small number of hyperscale providers now underpin banking, health records, government services and much of the communications sector at once, creating the same concentrated offshore dependencies beyond operators' control as diesel and vendor equipment. The difference is the scale of the consequences: a diesel shortage degrades backup power for the sites that need it, but the loss or compromise of a single cloud region can disrupt a shared service across multiple critical sectors simultaneously. The Australian market bears this out. The Australian Competition and Consumer Commission's final *Digital Platform Services Inquiry* report estimates that Amazon, Microsoft and Google together earned about 82% of Australian infrastructure-as-a-service revenue in 2023, against about 70% globally, and it points to high barriers to entry, limited interoperability and data egress fees that make switching providers hard.[36]

This concentration builds up through choices that make sense for each organisation. Consolidating on fewer technology platforms reduces complexity inside an operator, improves visibility and supports consistent security policy. However, when many operators make the same choice, the wider system comes to rely on a few providers, and a single failure can reach all of those operators at once. Interviewees described the same tension inside large networks. Centralised systems were described as easier to manage. However, as they noted, when a centralised system fails, the failure is large in scale, and redundant equipment does not contain a fault that every redundant component shares (Appendix D). Financial regulators provide examples of how this concentration risk can be addressed. The Australian Prudential Regulation Authority (APRA) asks regulated entities to consider concentration risk when selecting service providers, and to manage groups of providers whose combined impact is material.[62] The Financial Stability Board describes reliance by many institutions on one or a few providers as a systemic dependency.[63]

Australia's dependency is a strategic as well as commercial issue. Access to leading AI models has been interrupted before.[18] Sovereignty here is a question of who controls a capability, who is admitted to it and whose law governs it. Building the whole of that capability at home sits beyond Australia's scale. However, hosting a range of providers, and building the layers where Australian firms can compete, changes the terms on which access is negotiated, though interviewees differed on how far hosting alone amounts to sovereignty without local expertise and an allocation of that compute (Appendix D). The same pattern includes physical equipment, where hardware is bought abroad and then secured by a third party at additional cost.

Fragmented governance

Inside an organisation, the IT and OT divide is cultural before it is technical. The IT/OT convergence literature traces persistent differences between the two functions in hierarchy, risk tolerance and time horizon, and warns that separate security teams produce siloed views of what is in reality a single attack surface.[64] Yassine Maleh's 2021 analysis reaches for the term "non-governance": with responsibility for cyber security split across departments, risk that crosses those structures is managed by no one.[65]

That failure shows up as technical incidents. The ISA Global Cybersecurity Alliance, in its June 2025 guidance on applying information security standards to OT, records that pushing enterprise controls unchanged into OT can produce operator screen locking that creates unsafe conditions, antivirus products incompatible with OT equipment, patching that disrupts production schedules, and routine backup traffic that blocks safety control messages.[66] In each case, the control was reasonable in the environment for which it was designed and hazardous where it was applied.

The gap reaches boards as well. ASPI's 2019 study of critical national infrastructure finds that boards frequently lack the specialist expertise to interrogate OT cyber risk, and recommends they set and monitor an explicit risk tolerance for convergence rather than delegate the question downward.[22] Operators put it more bluntly to Dr Slay's independent review of the SOCI Act, telling the review that a focus on paperwork rather than intelligence-led practice itself risks creating systemic vulnerabilities, and describing compliance effort as document warfare rather than strategic uplift.[5] Minimum cyber training for board members was among the reforms survey respondents put first.

The same unevenness appears between sectors. Survey respondents rated governance as effective in a few sectors and weaker across the rest (Appendix C). Under the SOCI Act, the board or governing body of a responsible entity approves its annual risk management program report, so accountability for the program sits at the top of the organisation. Responsibility for managing the risk was often seen as dispersed. Interviewees described situations where the management of cyber risk moved between functions as lifecycle or dependency problems surfaced, so that the people accountable were not the people closest to the exposure (Appendix D). One interviewee noted that insurance is sometimes treated as a sufficient response. Insurance transfers the financial consequences of an incident, but the operator retains the operational consequences.

Colliding obligations

Fragmentation also appears between laws, and that is a different problem from the duplication the SOCI Act reforms are addressing. Duplication occurs when two laws require the same action. Obligations collide when two laws require incompatible actions.

The Department of Home Affairs has identified one such collision. Its 2026 consultation paper records that an entity captured by the SOCI Act may have continuous disclosure obligations under Chapter 6CA of the *Corporations Act 2001* or the ASX Listing Rules, while premature public disclosure of a cyber incident could alert the threat actor, encourage opportunistic attacks on similar systems elsewhere, and disrupt remediation being coordinated with ASD.[26]

The Department currently proposes to resolve this by creating a power for the Minister to direct an entity not to disclose, whose existence would then enliven an exemption from the listing rules on the basis that disclosure would breach a law.[26] Its 2026 feedback summary sets the mechanism at a maximum of 120 days, with insider-trading controls and consultation with ASIC and Treasury.[28]

A second collision is about money. Operators told Dr Slay's independent review that fixed regulatory funding cycles make absorbing ongoing changes under the SOCI Act difficult, with grace periods often falling mid-cycle, and that compliance costs arrive without a corresponding funding uplift.[5] For an operator whose revenue is set by an economic regulator under separate legislation, the obligation to invest and the ability to fund that investment sit under different statutes with different timetables. Survey respondents described the same collision (Appendix C). Where a service is delivered by a state entity, the obligation is understood poorly and funded reluctantly. Where regimes intersect, compliance sets the order of work. One remedy put forward by respondents is to let economic regulation account for future cyber risk alongside historical benchmarks.

Data used by AI systems is governed by more than one regime. The SOCI Act's definition of business critical data includes personal information about at least 20,000 individuals.[10] Respondents to the independent review said the breadth of that definition causes confusion and overlap with the *Privacy Act 1988*.[5] In its 2026 consultation paper on streamlining and modernising the SOCI Act, the Department of Home Affairs sought views on whether smart metering systems, meter data platforms and associated cloud analytics should be capable of capture under the SOCI Act.[6] An operator connecting AI to energy or water data may therefore need to meet both regimes. Guidance on how the SOCI Act and the Privacy Act apply together when operators use AI on energy or water data would help them meet both.

Supplier risk

The SOCI Act makes operators responsible for the security of equipment and services they did not build and cannot inspect. The enhanced risk management program rules made in June 2026 require the responsible entities for nine specified classes of asset to map their supply chains for major suppliers and critical components, to identify the maximum acceptable outage arising from a supply chain disruption, and to assess for every existing or proposed major supplier

the legal requirements that supplier is subject to, the sanctions or restrictions affecting its jurisdiction, and the access, influence and control it holds over the asset.[8]

One Australian instrument reaches further. APRA's prudential standard CPS 230, remade by determination in 2026, requires regulated entities to set tolerance levels for disruption to their critical operations and to manage material service providers under a register submitted to the regulator.[67] It binds the operator rather than the supplier, so it moves the obligation upstream without moving the accountability.

A 2021 comparative review by Topping and colleagues identified 14 cyber supply chain frameworks in authority and sector documents from the United Kingdom, United States and European Union, and reviewed the five most referenced in detail. It found that differing definitions and uneven coverage leave blind spots across vendors, integrators, contractors, procurement, disposal and foreign ownership, and that no single framework would support a detailed supply chain risk management program.[68]

The research base behind those frameworks is limited. Aarland and Gjøsæter's 2022 systematic review of digital supply chain security in the energy sector found 33 relevant papers in total, of which only two explicitly addressed supply chain attacks on critical infrastructure.[69]

Holding suppliers accountable therefore requires a standard that says what they are accountable for. Australia has not adopted a single standard, but the ISA/IEC 62443 standards family offers a workable solution: it distributes explicit lifecycle responsibilities across asset owners, integration service providers, maintenance providers and product suppliers.[20] Interviewees saw a single internationally recognised standard for OT as more useful than further national variation (Appendix D). Several said the volume of available guidance is itself an obstacle, and asked for guiding principles that help operators prioritise in environments where the first duty is safety.

Procurement is where that allocation is settled. Survey respondents put procurement alongside operations as the hardest stage at which to manage cyber risk, for reasons that are consistent: the decision is led by people without cyber expertise, cost and deliverability drive the decision, and equipment bought overseas cannot be verified to the degree everything else in the lifecycle can (Appendix C). A supplier's obligations are set or surrendered at that moment, so a standard that distributes responsibility across the lifecycle has to reach the purchase decision, and the operator has to be able to require it there. Supplier assurance also needs to address two dependencies: the small open-source components large systems rely on, and the small and medium enterprises inside critical infrastructure supply chains. A supplier standard reaches neither unless the purchase that brings them in asks for it.

Privileged access

Supplier risk is also carried by people, and personnel security is the one vulnerability in this chapter that the Australian regulator has tested. Survey respondents extended that risk beyond people, naming identity compromise, including the identities held by machines rather than staff, among the most significant vulnerabilities in Australia's critical systems.

The CISC reports, in its March 2025 guidance on the risk management program, that during its audit trials it found entities lacked appropriate insider threat mitigation and had insufficient policies in place to identify critical workers.[31] The Department of Home Affairs, consulting in 2026 on enhancements to the program rules, adds that existing mechanisms are not always applied across a whole organisation, and often perform general corporate functions rather than being targeted at personnel security threats.[56]

The risk concentrates where the workforce is contracted rather than employed. The *Annual Risk Review* records that temporary, contractual and externally provided staff often do not undergo the same vetting and security training as permanent employees, that contractors are frequently given trusted and privileged access, and that host organisations have limited control over how sensitive information is used once a contracted worker leaves.[9] Interviewees described the same exposure from the operator's side. Critical infrastructure networks can carry large numbers of third-party contractors, and they said controls that add complexity to a contractor's work are often resisted.

Legacy infrastructure

OT is built to last. A controller installed in the 1990s may still be running a pump today, because it works, and replacing it would mean stopping the service it controls. Long service life is a design objective. It also creates a vulnerability: assets designed for a working life measured in decades now face attacks developed in weeks, days or hours.[19]

Addressing vulnerabilities in OT is harder than in IT. Patching can require production outages that availability-critical services cannot schedule, vendor support for decades-old equipment lapses, and replacement is a capital program rather than a maintenance task.[66,21]

The vulnerability lies in a widening gap between what the threat environment demands and what OT can safely accommodate. The shorter exploitation timelines associated with AI widen that gap further.[24] Survey respondents put legacy systems at the top of the vulnerabilities facing Australian critical infrastructure (Appendix C), and interviewees explained why the gap keeps widening (Appendix D). Equipment specified years before it is installed can be out of support by the time a service begins. Replacing a fleet early to close a minor vulnerability was not seen as proportionate, so controllers with working lives of 15 to 20 years are kept running on compensating controls. Some interviewees saw technical debt as the defining problem in OT (Appendix D).

Capability

Capability covers what operators, government and industry are able to do, such as mapping dependencies, coordinating across sectors and recovering services, as well as the number of skilled people available to do it.

Evidence presented in this report shows gaps in both. Australian sources record a shortage of people who understand both IT and OT, and audits by the Auditors-General of Western Australia, New South Wales, Queensland and Victoria found gaps in how public entities and water providers manage cyber risk, including reliance on outside expertise that had not been tested.

The joint international *Principles of Operational Technology Cyber Security*, published in 2024 and authored by ASD with international partners, makes people one of six foundational elements, requiring OT-specific context, clear reporting routes and the authority to raise suspicious behaviour across IT, OT, engineering and field operations staff.[47] Maleh adds that capability must be mutual, because a workforce fluent in only one domain reproduces a governance silo at the level of individual judgment.[65]

Australian sources identify shortages in this capability. The *Annual Risk Review* states that training, capability and retention pathways remain insufficient to meet demand for skilled technical personnel, that the shortage is most acute in engineering and maintenance, cyber security and automation, and that it erodes the ability of operators to maintain, protect and modernise operational systems.[9]

Dr Slay's review identifies specialist shortages in OT security, identity engineering and supply chain risk management as a risk to the reform program itself,[5] and the TPDC's 2024 telecommunications resilience profile finds that Australia lacks sufficient telecommunications engineers and technical specialists to handle both legacy infrastructure and emerging technologies.[17]

Dr Slay's review also warns that smaller and regionally critical operators with limited internal security capability will need support and guidance to implement the reforms.[5] Australian audits bear that out. Western Australia's Auditor-General tested fifteen local government entities in 2021 using both control reviews and ethical simulated attacks, and found they had not managed their cyber security risks well: out-of-date software accounted for a large number of vulnerabilities, over half lacked controls to prevent staff falling victim to social engineering, and most lacked appropriate incident response and recovery plans.[70]

New South Wales shows the same pattern over seven years. In its 2025 review of its own audit series, the Auditor-General reported that only 24% of councils had trained staff in cyber awareness in 2019, rising to 74% by 2023 and falling back to 69% in 2024, with 45% running no phishing simulations at all in 2024.[23] Where agencies gave reasons for not meeting the state's minimum requirements, the most common were uplift programs still in progress or planned, then budget constraints; unfilled cyber security roles ranked well above skills gaps in current staff, which was among the rarest reasons given.[23] That describes a resourcing problem rather than a knowledge problem.

Queensland's Auditor-General found in 2024 that every entity it examined depended on people outside its own organisation for technical expertise during a cyber incident, and that none had tested those arrangements to confirm the third-party experts would respond in time. It noted that regional, rural and remote councils in particular could benefit from the state's central cyber security expertise, and that not all entities were aware of the services available.[71]

Two measurements are not yet available. A representative account of the Australian OT security workforce, covering its size, distribution, vacancy rates or capability, was not identified. Evidence about the condition of the equipment the workforce maintains is limited. The main source is the Victorian Auditor-General's 2019 audit, which tested control systems at four water providers over three days, excluding their corporate systems, and found that providers had invested in securing corporate systems while control system security lagged.[72]

Capability is therefore both unevenly distributed and unmeasured in OT, based on the evidence available. Survey respondents named workforce and skills most often when asked where investment is most needed, and rated workforce shortages the least significant of the vulnerabilities put to them. These responses emphasise skills and organisational roles over headcount. In interviews, where the cyber function sits was seen to shape what it can achieve, because a function sitting outside both technology and operations has to win each argument on business impact before it can act (Appendix D).

What this means

The vulnerabilities in this chapter are expressions of two drivers, convergence and interdependency.

Convergence has changed what can be reached. When OT was separate, an attacker usually needed to be physically present, and a control system could largely be secured by controlling the door. Connecting OT to IT, and through IT to the internet, removed that physical barrier. The equipment is now reachable, the people who understand it and the people who secure it sit in different teams, and the suppliers who maintain it hold access of their own.

Interdependency changed what a failure costs. A failure that once stopped at the operator now also moves to whoever depends on that service, and onward to whoever depended on them. That is what turns a local incident into a national one, and it is why the size of an operator is a poor guide to the consequences of its failure.

Every vulnerability in this chapter sits in one of these categories. Fragmented governance and privileged access are convergence problems, because they concern who controls the connection between IT and OT. Concentration, colliding obligations and supplier risk are interdependency problems, because they concern what an operator relies on and cannot control. Legacy and capability run across both.

Neither driver is currently visible. The modelling techniques to assess dependency exist. The national data needed to run them is not publicly available. Supplier accountability is expected of operators. A standard defining supplier responsibilities has not been adopted. Capability is required across operations, IT and governance. Its availability is limited and its distribution is unmeasured. The condition of OT equipment itself is unknown.



CHAPTER 4

The policy and regulatory landscape

The SOCI Act is the centrepiece of Australia's critical infrastructure regime. It covers eleven sectors and defines what assets within them count as critical.[10]

THE ACT IS under review at the time of writing. Dr Jill Slay's independent review of the Act was tabled in March 2026 and made six recommendations, drawing on written public submissions, surveys, roundtables with more than 600 participants, submissions from federal departments, and comparisons with the legislation of other countries.[5] The Government has accepted all six recommendations in principle and is responding in two tranches.[73]

Tranche 1 produced the enhanced risk management program rules, registered in June 2026, and a consultation on the Minister's directions powers. Tranche 2 is the broader program. The Department of Home Affairs set it out in a consultation paper, *Streamlining and Modernising the Security of Critical Infrastructure Act 2018*, which was open for feedback until 31 July 2026.[6]

This chapter examines Dr Slay's assessment of the Act, how governments designing their own regimes have judged the Australian model, and what the evidence shows about whether the regime is improving resilience.

How others regard the Australian model

The review's first finding is favourable. It concluded that the Act "has successfully established Australia as a global leader in critical infrastructure security governance".[5]

New Zealand reached a similar view from the outside. Its Department of the Prime Minister and Cabinet has been designing a critical infrastructure regime since 2023 and has compared its options against Australia's throughout. Its 2026 discussion document states that New Zealand "stands out from other advanced economies in not using dedicated legislative mechanisms to protect critical infrastructure from cyber harm", and places Australia alongside the European Union, the United Kingdom, Singapore and Canada in the group it measures itself against.[7] Its 2023 Cabinet paper names Australia among the jurisdictions moving toward a systems-based approach consistent with Organisation for Economic Co-operation and Development guidance, and observes that obligations can attach to an entity, as New Zealand's emergency management legislation does, or to critical assets, as the SOCI Act does, and that attaching them to assets "may be a better way to target expenditure" where an organisation delivers a range of services and only some are critical.[15]

What the review found, and what is being done

Dr Slay's review also criticises the Act, and stakeholder feedback was predominantly critical. The review reports that approximately 70% of sentiment towards the Act was negative, with complexity the dominant theme, that 118 of 230 respondents found the obligations unclear, and that 177 of 217 identified problems with its definitions, naming *critical worker*, *protected information* and the distinction between an asset and infrastructure as ambiguous.[5]

Home Affairs reports from the same survey that 55.6% of respondents identified overlaps with other frameworks, and names prudential standards, the *Privacy Act 1988*, the Defence Industry Security Program, the *Protective Security Policy Framework* and State frameworks as the prominent concerns.[6]

The review is careful about what those numbers mean. It records that there was no real philosophical disagreement with the need for the Act, that Home Affairs was seen as supportive and as responsive and agile in resolving problems, and that there was "a warmth towards the Department that is not displayed in the results attained".[5]

Enforcement is the subject of its second recommendation, which asks for a move from a light-touch compliance approach focused on administration and documentation to a penalty-based process with real enforcement of penalties.[5] The review's comparison of maximum penalties sets Australia's civil cap of AUD $11.1 million against the European Union's €10 million or 2% of global revenue for essential entities, the United Kingdom's proposed £17 million or 10% of turnover, Canada's proposed CAD $10 to 15 million and Singapore's SGD $1 million.[5]

The review's overall conclusion is that the Act's "complexity, regulatory overlap, weak enforcement posture, and gaps in addressing emerging threats necessitate comprehensive legislative restructure rather than further incremental amendment".[5]

A response to each criticism is under way. Home Affairs has published a response mapping reforms against all six recommendations, including an exemptions framework to reduce overlap where another law already imposes substantially equivalent requirements, stronger civil penalties, mandatory independent assurance, regulatory guides with worked examples, and new asset classes for space technology, data infrastructure, distributed energy resources, offshore electricity, and higher education and research.[6]

Coverage provides a good illustration. Space technology has been a named sector in the Act since the 2021 amendments, and Home Affairs states that because no operative asset classes have been prescribed, "the sector has no practical effect under the Act".[6] The risk management program rules already ask operators to consider the loss of positioning, navigation and timing systems as a material risk,[32] but until the proposed asset classes are made, the systems that support those services have no dedicated asset class. Survey respondents named the same gap: asked which dependencies are overlooked, they pointed to satellites and the positioning, navigation and timing services on which every other sector relies.

What has not been measured

Knowing whether the regulatory regime is working depends on collecting four kinds of evidence: that required programs exist, that controls are implemented and operating effectively, that services can continue through disruption and recover, and that national resilience is improving. Evidence of how well controls and services hold up also shows where they are weak.

Evidence that required programs exist, and what they cost, is well documented. The regulator received 457 annual reports covering 831 assets in 2023-24, each approved by the responsible entity's board or governing body where it has one.[31] The February 2023 impact analysis costed compliance with the risk management program obligations at $1.6 billion up front and about $1.1 billion a year across critical infrastructure nationally, a cost justified against the disruption it would avoid.[32] The independent review found that self-attestation by boards remains common, and suggested introducing an appropriately qualified expert into the process to provide external assurance.[5] The Department of Home Affairs' consultation paper on modernising the Act reports strong support for appropriately qualified external assurance.[6] Survey respondents questioned what that approval demonstrates, naming attestation without a technical basis among the most significant vulnerabilities in Australia's critical systems (Appendix C). The obligation assumes a capability the attesting body may not hold. Some interviewees argued that a board without technical expertise cannot attest to the security of its infrastructure unless a qualified engineer does that part of the work (Appendix D).

Whether infrastructure disruptions were indeed avoided has not been established. No Australian source was identified that measures whether outages have become shorter, recovery faster or cascading failures rarer since the obligations commenced.

Home Affairs says as much about its own assurance. The same consultation paper states that "regulator-led audits cannot provide broad assurance coverage across the regulated population in each reporting cycle", and that current settings can leave governing bodies without enough evidence to oversee security resourcing, risk appetite, dependency management and remediation decisions.[6] The Department proposes periodic independent assurance of whether a program is designed, implemented and operating effectively, on a base cycle of at least once every three years.[6]

Independent testing shows what self-assessment can overlook. In each of the adversarial tests of public sector cyber controls this report reviewed, the audit office found exploitable weaknesses. Queensland's Auditor-General used a third-party account to get past the controls of three public sector entities and obtained the highest level of access in two. Western Australia's Auditor-General phished fifteen councils, and staff at eight responded. When simulated attacks followed, nine councils never detected them and three took up to fourteen days, and all twelve of those councils had intrusion detection systems but no process to read what those systems produced in time.[70] The ANAO examined a department that had assessed itself as meeting the required standard on all eight core strategies and found it failing seven.[33] It found the same pattern at Defence, whose reporting it said indicated a more optimistic outlook than other internal documentation supported.[74] The New South Wales (NSW) Auditor-General found that NSW Health tested its incident response plan for the first time in October 2024, in an exercise that tested a third-party data breach rather than a failure of clinical systems, so it did not test what would happen if those systems went down.[75]

Adversarial testing by Australian audit offices is scattered across jurisdictions, covers a handful of entities at a time, concerns office systems far more often than the machinery running physical processes, and is mostly aimed at government bodies. National evidence from regulated entities consists mainly of self-assessment. Victoria is an exception: Part 7A of its *Emergency Management Act 2013* requires the operators of designated vital critical infrastructure to run exercises the Minister reviews and to submit to audits producing certificates and findings, with offences for non-compliance, and the Inspector-General for Emergency Management holds a statutory function to monitor and assess those arrangements. However, the Inspector-General's published reporting stopped after 2018.[35]

Repeated testing shows whether weaknesses are fixed. Victoria's Auditor-General tested industrial control systems in 2010 and found significant weaknesses, followed up in rail in 2016 and found little improvement, then tested live water systems at four providers in 2019 and again found significant weaknesses.[72]

One published independent assessment of a whole sector's resilience maturity was identified. The TPDC assessed the resilience maturity of Australian telecommunications as "developing", two on a five-point scale, drawing on consultation with 204 stakeholders and endorsement by a 26-member expert panel, and attributed the score largely to the early stage of resilience integration in federal policy.[17] Victoria publishes an annual account of its arrangements, its all-sectors resilience report, now in its tenth edition. These accounts describe activities rather than assess their effectiveness.[11]

The remaining gaps need more than regulation

Australia regulates critical infrastructure comparatively well. The weaknesses are documented and accepted, and reforms are in progress. The expert community surveyed for this report is less assured. No respondent expressed high confidence that current settings can address future cyber threats to critical infrastructure (Appendix C).

Dr Slay's recommendations show what is left to be addressed. Three of the six ask for something other than a change to the law: regulatory guides with worked examples, templates and plain-language materials; cross-agency work on AI, quantum computing, physical threat vectors and OT security; and stronger education and information sharing through the TISN.[5] Two further gaps sit outside the law. Survey respondents wanted an implementation playbook developed by industry (Appendix C). Australia also funds research on securing these systems, and interviewees saw no reliable route from that research into deployed capability and noted that critical infrastructure protection is not an established research priority here (Appendix D).



CHAPTER 5

Building national resilience

Building on Australia's regulatory foundation

THE SOCI ACT identifies critical assets, assigns obligations to responsible entities and provides an enforceable basis for managing risk. Australia's 2023 CIRS places that regulation within a broader national approach, combining an enhanced regulatory framework with collaboration through the TISN and the wider critical infrastructure community.[49] Regulation and resilience therefore perform different but complementary functions.

The *Security of Critical Infrastructure Legislation Amendment (Enhanced Critical Infrastructure Risk Management Program) Rules 2026* show how these functions can work together. The rules require specified entities to map major suppliers and critical components, identify the maximum acceptable outage caused by supply chain disruption, and meet a segregation standard under which critical services continue for at least three months while connected systems are restored.[8] The SOCI Act attaches these requirements to an entity that can be held accountable, while the requirements themselves concern the continuity of a service during disruption.

Infrastructure Australia explains why the distinction matters. Asset protection concerns the performance of individual infrastructure, while resilience concerns the capacity of assets, networks, places and communities to withstand, adapt to and recover from disruption.[50] Applying that systems view would complement the SOCI Act by showing how regulated assets combine to provide critical services, what those services depend on, and how failure could spread across organisational and sector boundaries.

From critical assets to critical systems

A resilience assessment begins with a service that must continue, then identifies the functions that produce it, the systems on which those functions depend, the consequences of losing them and the alternatives available during disruption. This reverses the asset-first view identified earlier in this report: assets remain subject to regulation, but their importance is assessed through the services and systems they support.

ASD's *Principles of Operational Technology Cyber Security* provides an Australian-led method for applying this approach within an organisation. The document, co-designed with Australian critical infrastructure operators, asks organisations to identify the OT systems needed to continue critical services, understand the physical process each system controls, and map dependencies within and beyond the OT environment.[47] For electricity generation, this means identifying the generator, controller and suitable fuel supply as the minimum system required to produce electricity, which gives the operator a practical basis for deciding what must be protected, sustained and restored first.

Infrastructure Australia's *Resilience Principles* extends the same reasoning beyond the operator. The framework requires infrastructure decisions to consider assets and networks alongside the places and communities that rely on them, because the failure of one asset can increase consequences for other services, economies and the environment. The method therefore addresses cascading effects by tracing what depends on an asset and planning how the affected services will continue.

The TPDC has demonstrated how this analysis can be applied across a sector. Its *Australian Telecommunications Sector Resilience Profile*, developed with 204 stakeholders and a 26-member expert panel, assessed the resilience maturity of the sector as a whole, including providers and governments at local, state and federal levels.[17] Applying the same process across other critical infrastructure sectors would identify shared dependencies and service thresholds, while connecting the sector profiles would provide a national view of risks that no asset register can show, a step Victoria has taken within its own borders annually since 2015.[11] Interviewees also put mapping first, with socio-technical mapping of critical infrastructure as the practical starting point, and noted that responsibility for applying the method has not yet been given to a department (Appendix D).

Building capability through practice

Resilience treats workforce capability as the capacity to operate and recover the service, rather than the number of cyber specialists employed. ASD's principles require process engineers, cyber personnel, field staff, suppliers and decision-makers to understand the physical process and practise incident, continuity and recovery arrangements together, while the ACSC exercise program already tests strategic, operational, technical and communications capability with critical infrastructure owners and operators.[2] ASPI recommends extending that program through OT scenarios, executive war-gaming, technical red-team testing and wider participation across critical infrastructure providers.[22] This approach complements regulation by testing whether the people named in a plan can sustain and restore the service under pressure. Experts and practitioners locate resilience in the same place (Appendices C and D). Interviewees described a standard as setting a boundary, and saw much of what builds resilience as organisational, sitting on top of technical capability. In their experience, plans are rarely followed exactly, and their value lies in rehearsing the problem in advance so that departures from them are recognised quickly. Testing therefore needs to reach the people who would implement the plan, and is most useful against a defined limit, such as the longest outage a service can tolerate (Appendix D).

Assigning responsibility for the system

Australia has several models for assigning the responsibilities that sit between regulated entities. The CIRS gives industry responsibility for the infrastructure it operates, gives governments responsibility for national and jurisdictional settings, and uses the TISN for sector and cross-sector collaboration, but specifies that the TISN has no operational role. The TISN's current framework has sector groups under industry and government co-chairs and cross-sector workstreams with named leads.[27]

The Strategy's companion *Resilience Plan* adds delivery accountability: the CISC supports the delivery of every activity in partnership with the Critical Infrastructure Advisory Council, the Resilience Expert Advisory Group and TISN members, and those partners evaluate the Plan's deliverables annually.[16] The New South Wales *Critical Infrastructure Resilience Strategy* keeps primary responsibility with owners and operators within a non-regulatory partnership involving governments and communities.[76] The TPDC uses a more formal cooperative model, bringing providers, regulators, governments, dependent services and community representatives into a common sector assessment, although its telecommunications profile also identifies that the benefit of shared resilience work reaches operators who do not contribute to it, alongside fears of anti-competitive behaviour and enterprise-level decisions that are rational without producing sectoral resilience, which can prevent voluntary cooperation from resolving shared risks. New Zealand's 2023 Cabinet paper proposes a different approach by assigning ministers and agencies clear responsibility for the resilience of the whole critical infrastructure system.[15] Delivery of the Strategy's activities therefore has owners and an annual evaluation, but whether the system's outcomes are improving, in shorter outages or faster recovery, is a question none of these arrangements asks. These models offer Australia a choice between stronger sector cooperation, clearer public accountability, or a combination in which government owns system-level risks and providers retain responsibility for operating assets and services. The evidence points to sector-level bodies that receive incident reports, share intelligence across sectors and with overseas counterparts, and pass it to operators, on the model already working in banking (Appendix C). The evidence also identifies an action government can take now. Interviewees observed that where regulation has created a coordinating centre and made clear that competitors may work together, cooperation has followed (Appendix D). Permission and convening are therefore design choices available to government, and they address some of the barriers to shared resilience identified here.

Applying existing approaches nationally

Australia does not need to develop a national resilience framework from first principles. The CIRS provides the national policy foundation, the TISN provides an established collaboration network, and the SOCI Act provides enforceable obligations. The *Principles of Operational Technology Cyber Security* provides operational guidance that can be applied within regulated entities, while Infrastructure Australia's *Resilience Principles* provides the broader systems and community view.

The United Kingdom National Cyber Security Centre's *Cyber Assessment Framework* provides a method for converting resilience principles into assessable outcomes. Its four objectives and fourteen principles allow an oversight body to set a target profile for a sector, add outcomes suited to that sector, and assess whether essential functions can continue and recover.[34] The TPDC profile provides an Australian sector-level application, establishing a baseline across resilience principles, capabilities and resources that can be repeated to measure progress.

Together, these approaches provide the elements needed for national application: identify the critical services that must continue, map the systems and dependencies that produce them, set outcomes suited to each sector, assess the capabilities needed to meet those outcomes, and repeat the assessment as systems and risks change. The evidence reviewed for this report does not show whether this process has been applied consistently across Australia's critical infrastructure sectors, or whether applying the frameworks has prevented outages, maintained critical services or improved recovery. A 2026 review of the field states the absence: there is no standardised set of resilience metrics widely adopted in Australia's energy sector, and without them it is difficult to quantify the benefits of hardening or to set engineering targets for recovery times.[77] Any national application should therefore define its intended outcomes at the outset and collect the evidence necessary to evaluate each framework's effectiveness.

Bringing the approaches together

Australia's critical infrastructure regulation provides a necessary foundation for national resilience. Applied asset by asset, it shows the dependencies of one asset at a time rather than those of the service the assets deliver. Existing resilience approaches address that gap by starting with the service, identifying the systems and people that sustain it, testing whether they can operate through disruption, and assigning responsibility for risks that cross asset and organisational boundaries.

Australia can apply ASD's operational guidance within regulated entities, use the TPDC's method to assess resilience across sectors, and connect those assessments through the CIRS and the TISN. The same approach applies to digital and AI infrastructure, which is recognised as critical only in part: recognising it as critical, mapping the services that depend on it, and assigning responsibility for its resilience. Recognition should also extend to national planning and investment, so that digital and AI infrastructure, including national supercomputing, is funded as long-term national infrastructure. Clear public responsibility will still be required for system-level risks that voluntary cooperation does not resolve, but this can be added without displacing the operational responsibilities established by the SOCI Act. Used together, these arrangements would strengthen the resilience of the critical operational systems on which Australian communities depend.



Appendices

APPENDIX A

Steering Committee

The project was overseen by a Steering Committee of Academy Fellows and Fortinet representatives, chaired by Kelly Bayer Rosmarin.

Member	Position	Organisation
Kelly Bayer Rosmarin FTSE (Chair)	Chief Executive Officer	Australian Unity
Professor Emily Hilder FTSE	Head, Advanced Strategic Capabilities Accelerator	Defence Science and Technology Group
Professor Shazia Sadiq FTSE	Data Engineer and Director	The University of Queensland
Professor Joanna Batstone FTSE	Adjunct Professor (Practice)	Monash University
Professor Maurice Pagnucco FTSE	Professor	UNSW Sydney
Dr Sue Keay	Director, UNSW AI Institute	UNSW Sydney
Professor Jay Guo FTSE	Director, Global Big Data Technologies Centre	University of Technology Sydney
Dr Ian Oppermann FTSE	Commissioner	Australian Competition and Consumer Commission
Nicole Henry	Head of Government Relations (ANZ)	Fortinet
Andrew Stevens	Director, National Public Sector	Fortinet
Michael Murphy	Director, Operational Technology and Critical Infrastructure	Fortinet

APPENDIX B

Literature review

The literature review was the first of the project's three evidence streams, ahead of the discovery survey and the interviews. The review assembled, verified and organised the published evidence on: the law and the rules that define and govern Australia's critical infrastructure, the national threat picture, the engineering literature on OT, the research on interdependency and cascading failure, the regulatory approaches of comparable jurisdictions, and the independent audit record of how Australian entities perform in practice when their cyber resilience is tested.

The review also had a second purpose, which shaped the survey and the interviews that followed: to identify gaps in published evidence that the project would need to address.

Search strategy

Multiple rounds of organic search were undertaken over about 14 weeks to identify relevant sources across several themes. AI-assisted search tools were used to help identify sources for retrieval under researcher supervision. A copy of each source was saved and documented. Every source was read and reviewed by the researchers involved, with its URL and bibliographic details recorded, and sources that did not meet the evidence standard on review were excluded with the reason noted.

The first round of search covered five theme areas: the Australian policy and regulatory framework; the cyber threat landscape, with an Australian focus; operational technology security and secure-by-design; systemic vulnerabilities and cascading risk; and international comparators, covering the European Union, the United States, the United Kingdom and New Zealand.

A second round added a sixth theme, assurance and audit evidence, once it became clear that the performance audits of the ANAO and the state and territory auditors-general formed a distinct source of evidence about practice. It also sought resilience and assessment material the first round had missed, at both the national and the state and territory level.

A third round closed gaps by sector, adding sources on sector-level risk assessment, the regulation and guidance specific to individual sectors, and the public record of incidents within them.

A fourth round was undertaken to ensure the SOCI Act and its reviews and reforms were properly captured, adding sources on the legislative history of the Act and on the scrutiny, consultation and post-incident review that have shaped it.

A fifth round closed the gap on how Australian jurisdictions organise for resilience, adding sources on the resilience arrangements of the Commonwealth, states and territories, and on operational resilience obligations in regulated sectors.

A final update added sources identified through Steering Committee review of the drafts, extending coverage to AI security and sovereign AI capability, concentration in the cloud market and third-party risk, the resilience of emergency communications, and updated OT security guidance.

Evidence base

Across all rounds 194 sources were identified and reviewed. 10 did not meet the evidence standard on review and were excluded. The review included 184 sources: 67 on the Australian policy and regulatory framework, 23 on the cyber threat landscape, 22 on OT security, 37 on systemic vulnerabilities and cascading risk, 18 on international comparators and 17 on assurance and audit.

The evidence base is weighted towards authoritative sources: 71 were published by Commonwealth departments and agencies, 18 by independent statutory authorities and regulators, 14 by state and territory governments, 27 by international governments and regulators, 15 in academic outlets and 15 by statutory corporations, parliamentary committees, universities, learned academies and standards bodies. The remaining 24 are industry, vendor, consultancy, think-tank and media sources. These are used for threat data, accounts of specific incidents and policy argument not available from official sources.

By form, the largest groups are risk advisories and assessments (23), regulatory guidance (22), frameworks, standards and maturity models (19), independent audit and review reports (18), strategies, policies and plans (16), peer-reviewed articles and conference papers (15), legislation and legislative instruments (11) and threat intelligence and annual threat reports (11). The base is current: 134 of the 174 dated sources were published between 2024 and 2026.

Coverage by sector reflects the review's cross-cutting questions. 42 sources take a single SOCI Act sector as their subject, 41 treat all sectors, and 101 are sector-neutral frameworks, standards, comparators and research. Sector-specific coverage rests substantially on the sector risk advisories. Beyond them, communications is the most covered sector and space technology the least.

Three features of the evidence base shaped the report. Most of the strongest material describes rules: legislation, guidance, standards and strategies establish what is required. No Australian source identified measures whether the state of entities' controls predicts their outcomes; the links that exist are single cases. Evidence of practice is concentrated in a small number of independent audits and the national threat reports. Audit offices have adversarially tested controls in three states, and auditors have tested controls themselves in two more jurisdictions and the Commonwealth. Only one test covered OT and a privately owned operator, Victoria's 2019 audit of water control systems, and the audits' most consistent finding is that controls are asserted and not tested. Finally, the published record contains no primary fieldwork on the operation of Australian critical infrastructure, and incident and threat data are largely sensitive and unavailable.

The literature review also documents varied state and territory arrangements. New South Wales, South Australia and Victoria have each published a critical infrastructure resilience strategy, and among the states and territories Victoria alone has a statutory regime under which designated operators must exercise and be audited. Queensland and Tasmania address critical infrastructure through their disaster risk and emergency management arrangements; Queensland's define it and Tasmania's do not. The record of the 2026 SOCI Act reforms runs from review to registered rules for the enhanced risk management program, which allows the report to consider their implementation as well as their intent; the ministerial directions amendments and the second tranche remain at consultation.

The report's 77 endnotes cite 93 of the 184 sources. Sources read and not cited have informed the framing and organisation of the report.

APPENDIX C

Survey

The purpose of the discovery survey was to establish, early and across a broad expert base, which systems and dependencies matter most, which threats and vulnerabilities are judged most serious, and where the people closest to the problem think effort should go. The instrument was developed with input from the Steering Committee, and distributed online between 2 July and 1 August 2026. It asked 28 questions: a short profile, rating grids on sector criticality, threats, governance and vulnerabilities, and a series of open questions on priorities, investments, collaboration and emerging risks.

36 people responded, of whom 20 completed the full survey and 16 answered it in part. 11 of the 16 partial responses stopped at or before the profile questions, so the number of responses is 21 to 24 for rating questions and 8 to 19 for open questions. Every figure in this summary and in the report body is given as a count of those who answered that item, with "don't know or not applicable" excluded, because the base varies from question to question. These are counts of responses, not estimates of prevalence, and the report uses them as such.

Most respondents have a research background. 19 of 36 described their perspective as academia, 10 as industry, 4 as other, 2 as government and 1 as not-for-profit, and 20 of 36 had worked in their field for more than 20 years. Asked which contexts their experience covered, 21 named higher education and research, 13 communications, 12 data storage or processing and 7 the defence industry; energy was named by 4, healthcare by 5, transport by 2, water by 1 and food and grocery by none. The results therefore carry an informed, experienced and largely academic view of the problem, with the operator and regulator voice less prominent.

Which systems matter, and why

Respondents were asked to rate the importance of each critical infrastructure sector to national resilience and then to choose the single reason it mattered most. On importance, energy was rated extremely important by 23 of 24, communications by 20 of 23, water and sewerage by 18 of 22, healthcare by 17 of 22, food and grocery and transport by 16 of 22 each, data storage or processing by 14 of 23, financial services by 12 of 21, higher education and research by 9 of 22 and space technology by 6 of 22.

For five of the ten sectors the most-chosen reason a sector matters was its interdependency with other systems: data storage or processing (13 of 23), communications (12 of 22), energy (11 of 24), higher education and research (10 of 22) and transport (8 of 22). For healthcare (15 of 22), water (12 of 22) and food and grocery (9 of 22) it was the potential loss of life; for financial services the impact on the economy (13 of 22); and for space technology national security (14 of 19). When experts explain why a sector is critical, they reason about what depends on it and who would be harmed if it stopped.

Threats, and which are underestimated

Six threat types were rated for significance to critical infrastructure. AI-enabled attacks were rated very or extremely significant by 21 of 24, ahead of state-sponsored activity (17 of 23), cybercrime (17 of 24), supply-chain compromise (16 of 23), firmware issues (15 of 23) and hardware tampering (10 of 23). Asked which of the same six were underestimated, respondents gave different ratings. Firmware issues were considered underestimated to some degree by 20 of 20 who answered, supply-chain compromise and hardware tampering by 19 of 20 each and AI-enabled attacks by 19 of 21, while cybercrime, the most familiar of the six, was thought very or extremely underestimated by only 2 of 21. AI-enabled attacks (11 of 21) and supply-chain compromise (10 of 20) led on the stronger measure of very or extremely underestimated.

The open responses reinforced the pattern. State-sponsored activity and espionage were the other threats most often named as underestimated, and when asked about emerging risks, 8 of 15 named AI and 5 named quantum computing, with insider threat and the shortage of skilled people also mentioned. One respondent argued that AI does not necessarily make well-resourced state actors more capable. However, it lowers the cost and competence needed to mount an attack, and so, in the respondent's words, "introduces entirely new actors".

Vulnerabilities

Seven candidate vulnerabilities were rated by respondents. Legacy systems were rated very or extremely significant by 18 of 20, then information-sharing gaps (12 of 20), integration of IT and OT (11 of 17), governance issues (11 of 20), supply-chain assurance (10 of 19), regional infrastructure constraints (10 of 18) and workforce shortages (9 of 20). Asked in their own words for the single most significant vulnerability, respondents named legacy systems, foreign dependence in hardware and software, the absence of a clear system-wide plan and of national leadership, board self-attestation without a technical basis, identity compromise including non-human identities, and, in one respondent's words, that few of those responsible could say who they depend on or who would be affected if they failed.

Asked at which stage of the asset lifecycle cyber risks are hardest to manage, 9 of 21 chose operations and 8 chose procurement, with maintenance, deployment and decommissioning chosen by 4 between them. The explanations for procurement were consistent: procurement is led by professionals without cyber expertise, cost and deliverability drive the decision, and the security of equipment procured from overseas cannot be verified to the same degree as anything else in the lifecycle. Several respondents put the point in terms of sovereign capability, describing Australia as dependent on foreign providers at every level of the stack.

Governance, and confidence in the policy settings

Respondents rated how effectively each sector is governed and regulated for cyber resilience. Defence (15 of 21), financial services (14 of 21) and energy (14 of 22) were most often rated effectively or better; food and grocery (8 of 21) and transport (7 of 21) least often. No sector was rated better than "effectively" by a majority. The explanations were more pointed than the ratings. Where services are provided by state governments or state-owned entities, respondents reported poor understanding of the SOCI Act's requirements and reluctance to fund a response; where regulatory regimes intersect, especially with the financial sector, priorities are set by compliance rather than by risk; and governance was described as patchy across sectors, producing short-term political responses when problems occur rather than systemic review.

Asked how confident they were that Australia's current policy settings can address future cyber threats to critical infrastructure, none of the 15 who answered expressed high confidence. Three described the settings as a strong foundation that must evolve faster than it does, or as broadly on the right path, and one said government was addressing the problem to some extent. The remainder expressed little or no confidence, citing a lack of teeth, policy that is not clearly articulated, under-investment in long-term concerns and, in one case, that resilience should be planned on the assumption that an attack will succeed.

What respondents would do

The open questions on reform, investment and collaboration produced a consistent set of themes. On reform: minimum cyber training for boards; agreements between the Commonwealth and the states so that state entities are prepared to adopt federal settings; economic regulation of infrastructure entities, especially in energy, that allows for the costs of managing future cyber risks, rather than relying on historical benchmarks; enforceable cross-sector benchmarks; and sector-level bodies that receive incident reports, share intelligence with one another and with overseas counterparts, and pass that intelligence to operators, on the model respondents saw working in banking. On investment: workforce and skills were named most often, then secure supply chains and a trusted computing base, protection of the small open-source components on which large systems depend, modernisation of legacy systems, and quantum-resistant capability. One respondent observed that standards on their own are a fence around an organisation rather than protection, and another that cyber resilience is not only a technical problem, since much of what builds it is organisational and sits on top of technical capability.

On collaboration, the strongest themes were real-time threat-intelligence sharing and joint exercises, sovereign capability, an industry-developed playbook for implementing the SOCI Act, and collaborative rather than adversarial responses when problems arise. Asked what should be scaled or replicated, respondents pointed to regional threat-sharing hubs and cross-sector incident exercises, cooperative research programs, and a domestic equivalent of the security grants that Australia funds abroad.

What is overlooked

Two questions asked what is missing from the discussion. On dependencies, respondents named satellites and the positioning, navigation and timing services on which every other sector relies; the measurement and timing infrastructure behind power-system situational awareness; the small open-source projects that sit beneath important systems; and the extent of dependence on foreign digital infrastructure. Water was described more than once as underestimated in its effect on other sectors, and waste, and electoral systems and democratic discourse, were each suggested by one respondent as missing from the list of sectors. A final comment noted that small and medium enterprises face greater cyber risk than large operators and often form part of critical infrastructure supply chains, so that their compromise reaches beyond the firm itself.

How the report uses these results

The report draws on the survey where a result supports or develops a finding established by other evidence, and attributes each use to the survey; the counts behind each statement are given here.

APPENDIX D

Interviews

Interviews were held with 10 experts, balanced between strategic and policy perspectives and the experience of industry and practitioners. Participants included people responsible for cyber security in organisations that run OT at scale, people who advise government on critical infrastructure and its regulation, people with senior experience running large networks, people who support operators with threat intelligence, and people working in national security and technology policy. The interviews also included a research and engineering perspective on how these systems are secured in practice. The conversations covered what participants judge the main challenges to be, how disruption travels between systems, where accountability sits, and what they would change. All interviews were organised and led by ATSE. Interviewees were identified by members of the Steering Committee, and a member of the Fortinet team was invited to attend them, reflecting the joint nature of the project. Interview participants were provided with information about the interviews in advance, including who was attending, the purpose, and how the interview results would be used in the report.

Interconnection and the limits of isolation

The most consistent theme arising from the interviews was that the degree of interconnection between systems is not well understood, particularly where connections involve third parties. Interviewees described decisions taken without a clear view of what depends on the system being changed, and the difficulty of establishing who would be affected if a service stopped.

Interviewees were also clear that isolation is not available to many operational systems. Diagnostic equipment, communications infrastructure and transport systems need external connectivity to perform their function, and the vendors who support them need access for as long as the equipment is in service. One interviewee went further, describing a control that prevents a machine from performing its function as itself a form of denial of service.

Views diverged on how far IT and OT can be kept apart. For an operator running its own control systems, the view was that critical OT assets should be kept fully separate, with their own resourcing and segregation of duties, and that convergence should mean only the point where the two networks meet. Losing visibility of a control system can have physical consequences. From the perspective of large networks, where every service runs over IP and much of the OT sits in public cloud, physical separation is generally not possible. Protection there has to stop an intruder who reaches one site from moving across the whole network.

There was more agreement on how to manage the risks of connectivity, by planning the protective layers between an exposed point and a critical asset through segmentation, restricted remote access, attack surface reduction and observability. Several favoured simple and visible controls. A physical authorisation step on vendor access, for example, achieves what more elaborate provisions reach for in a form that operators and regulators can both understand.

Dependence on communications networks was raised repeatedly. Several interviewees described operations that rely on mobile networks at their sites, where a single carrier does not always cover every location. One interviewee noted that most telecommunications outages, by number and duration, begin with a loss of power, particularly in regional and remote areas where networks rely on the grid. The dependency is also not reciprocal. When a large provider has difficulty, the organisations relying on it have difficulty too, and they have little standing to ask for anything in return.

To keep services running when power or communications fail, some operators give their energy provider a priority list of critical sites to restore first, keep portable communications equipment that can bring a site's telemetry back online, and give critical workers access to more than one mobile network. Satellite services fill some gaps. However, the view was that satellite capacity is limited, because a small number of satellites covers the whole country and each beam serves a very large area, so satellite is unlikely to carry all traffic if terrestrial networks fail.

Dependence on a few providers was expected to extend to space. As one interviewee saw it, the investment needed for low earth orbit constellations is likely to leave the market to two Western providers, and Australia is a small participant in that market. A capability shared with partner governments was suggested as one option, with funding and management the main difficulty. Capacity to repair submarine cables was also raised as a further concern.

Interviewees cautioned that redundant equipment does not protect a network from a fault that every redundant component shares. Large network outages have come from a common fault spreading through the network, even where redundant equipment was in place. Centralised systems are easier to manage. However, when a centralised system fails, the failure is large in scale.

Several interviewees framed interconnection as a single system. On this view, IT and OT form one technical system that boards and executives need to understand as such, and socio-technical mapping of critical infrastructure is the first practical step. The method exists. However, an interviewee noted that responsibility for applying the method has not yet been given to a department.

Legacy systems and the pace of change

Much of this infrastructure was built decades ago and now runs alongside newer technology. Systems cannot be patched or taken offline at will, and in continuous operations there is little or no scheduled downtime, so a small change requires substantial planning because of what depends on it.

Lifecycles were a consistent theme. Interviewees described equipment specified in one decade, installed in the next and unsupported by the time services began. Controllers with service lives of 15 to 20 years are managed through virtual patching and compensating controls, since replacing a fleet well ahead of schedule to close a minor vulnerability is not proportionate. Work in these environments is delivered as projects, and they noted that a new project does not always account for the systems that depend on the infrastructure it touches. For some, technical debt is the defining problem in OT.

Funding runs on a different cycle again. In multi-year programs, interviewees said, assets can reach end of life before money is released, so the recorded risks change while the funding case is still being developed. Design is improving where security is considered from the start and becomes a line item in the build. The aim, as one interviewee described it, is security built into operations, with neither placed above the other. Retrofitting an existing site is harder and is decided on a benefits analysis.

Governance, ownership and skills

Cyber risk was consistently framed as a governance question. Interviewees agreed that chief executives are accountable for cyber risk. Several found it harder to establish who mana ges that risk in practice, as accountability moves between functions when a lifecycle or dependency problem surfaces. Senior appointments are rarely made with a cyber remit, so the people formally accountable are not usually the people closest to the exposure. An interviewee described making operations responsible for enforcing security measures and the cyber function accountable for them, which gave the two functions a clear basis for working together.

In interviewees' experience, where the cyber function sits shapes what it can achieve. When the function reports outside both technology and operations, much of its effort goes into explaining risk in business terms to people focused on keeping the service running. Cyber teams often translate cyber risks into the organisation's enterprise risk framework, in executives' terms, so that executives can decide whether to accept each risk. Interviewees described presenting the same material to audit and risk committees, executive teams and boards, and said the presentations do not always lead to investment. Some noted that outside consultants' advice can be given the same weight as the organisation's own teams, and that insurance is sometimes treated as a sufficient response to cyber risk.

Capability at governance level came up in several interviews. Boards are weighted towards legal and financial backgrounds, and technical literacy varies. The capability now needed spans IT, OT and AI together, and is scarce at that level. Advanced detection skills, one interviewee observed, sit mostly in government and the finance sector, and many organisations use advanced security tools only for basic logging. Others noted that organisations calibrate their priorities to the signals they receive, including public statements about risk, so what is said publicly shapes where effort goes. Some argued that a board without technical expertise is not able to attest to the security of its infrastructure unless a qualified engineer does that part of the work. Middle management was also identified as part of the gap, where senior understanding of the complexity is not always translated into practical programs and decisions.

Understanding across government was described as uneven, stronger in some areas than others. Interviewees valued direct engagement between the people who operate these systems and the people who set rules for them, and several said that engagement is inconsistent. The view was that government also needs more people who understand the industries it oversees, so that it can assess and rank risk across sectors with industry supplying its view. Hiring arrangements and clearance requirements make it harder to bring external expertise into government. The regulator faces the same capability question, with policy expertise needing technical expertise alongside it.

Awareness inside organisations was raised as a distinct problem. Users take the path of least resistance, and where the secure route is slow or unfamiliar they find another, such as moving data off an operational system on removable media. Large numbers of contractors move through these networks and resist controls that add complexity to their work. The view was that periodic campaigns are not enough on their own, and that awareness programs need to reach executives and engineering teams as well as general staff. One interviewee wanted operations staff to report equipment breakdowns to the cyber team, since a fault at one site may share a cause with faults elsewhere. Change is difficult even for organisations that have experienced an incident.

Standards, guidance and coordination

Interviewees work to several frameworks at once and saw the volume of guidance as an obstacle in itself. Detailed frameworks, they said, generate more questions than answers for people working directly with operational systems, and operators want guiding principles to help them prioritise. Because standards give a direction and leave the method open to interpretation, a large organisation needs one agreed source for interpreting them. Standards written for IT also do not transfer cleanly to environments where the first duty is safety, and the view was that a single internationally recognised standard for OT is more useful than further national variation. Some went further and argued for narrower regulation, supported by a rulebook for accreditation and an industry-based peer review of how operators meet it.

Interviewees described limited professional networks in some fields, and knowledge sharing that depends on individuals more than on institutions. They said that industry events are often weighted towards vendors. Views aligned on the value of regular forums held under the Chatham House Rule, where operators can describe what they have actually done, including their failures, which otherwise often go unreported. Some suggested government could encourage or require that sharing. Vendors were still a useful source of information that operators do not get elsewhere, such as supply timelines and hardware availability.

Where sharing works, it works well. Interviewees valued the anonymised national threat intelligence capability as an unusual strength, one that improves as large operators contribute their own network visibility, and the protection that allows an organisation to work with the national agency during an incident without that cooperation being turned against it. An interviewee pointed to a sector that coordinates effectively because regulation gave it a coordinating centre and, as importantly, permission for competitors to work together. On that view, the federal role is to grant permission and to convene, since organisations will coordinate where they are confident that doing so is allowed.

Interviewees also distinguished intelligence from information. Intelligence, one explained, tells the recipient what is happening and what to do next, and so prompts action. Many organisations do not have the capability to take in government threat feeds directly, and need an intermediary step that turns threat information into guidance they can act on.

Interviewees were realistic about response plans. Plans are rarely followed exactly in an incident, and their value lies in thinking a problem through in advance, so that departures from the plan are recognised quickly. One interviewee argued for setting the longest outage a service can tolerate, designing for it and testing against it. Testing a failover carries its own risk, the interviewee noted, because a failed test causes an outage, and learning from other operators' failures helps.

AI and dependence

Views on AI varied more than on any other subject. Some interviewees pointed out that the underlying techniques have been in use for decades, that defensive use has reduced compromise, and that attacks on control systems have run for two decades with well-understood methods. For them, the more pressing issues were the understanding of the people who now act on machine-generated advice in operational settings, and mapping the systems. Others saw AI as amplifying existing exposure, which keeps hygiene, attack surface reduction and observability at the centre of defence. Concern was greater about the near term, where capable models could give attackers a material advantage. A further concern was that AI has raised the number of vulnerabilities found beyond what many organisations can prioritise, at a time when the quality of overseas vulnerability data has declined, so operators need help deciding which vulnerabilities matter to them.

Others raised a concern about concentration. A small number of models, trained in similar ways, sit beneath a growing number of systems. The organisations using them see an interface. The training data, the evaluations and the safeguards are not visible to them. A fault in one model could surface across many sectors at once. Concentration among a small number of providers creates a policy dependency alongside the technical one.

Access was described as a strategic exposure. Interviewees noted periods when access to leading models was restricted, and said the exposure grows as these systems are relied on more heavily. Sovereignty, in their terms, means who controls a capability, who has access to it and whose law applies to it, a separate question from the domestic legal settings that affect what models can be trained on. Frontier-scale development was judged unrealistic in Australia. Interviewees saw the achievable strengths as compute capacity and the application layer, with hosting for a range of providers improving both resilience and Australia's position when negotiating access. Several described the objective as managed interdependence, built on being useful enough to partners that access is not withdrawn.

On coverage, interviewees distinguished the facilities from the models that run on them. Reforms are expected to widen coverage of data storage and processing, and on this view the models themselves are approaching the point at which they warrant similar treatment. One interviewee added that obligations are also uneven. Operators are required to report incidents, and the providers of the models they depend on have no equivalent obligation. Other jurisdictions are moving to require monitoring and reporting from those providers.

Interviewees also described the weakening of geographic protection. Assets that were secure through obscurity are exposed as automated scanning lowers the cost of finding vulnerable systems, and capability varies widely between the organisations responsible for infrastructure at local and regional level.

Research and domestic capability

Interviewees returned to what Australia can build for itself. Examples ranged from running AI workloads on domestic hardware to computing research under development here. Hosting compute for overseas providers was not seen as sovereignty on its own, because local firms also need the expertise and an allocation of that compute. The achievable strength, several said, lies in the compute and application layers, where Australian companies can build on what others provide.

An interviewee pointed out that Australia funds research on securing these systems, and that a reliable pathway from that research to a deployed product is not yet in place. The same interviewee saw critical infrastructure protection as not yet an established research priority in Australian universities. Clean energy equipment, for example, is bought overseas and then secured by a third party at additional cost. Domestic work on securing that equipment exists and does not reach the market.

What interviewees would change

Interviewees converged on a short set of changes. For operators, they wanted guiding principles to help them prioritise, awareness programs that reach executives and engineers, board capability spanning IT, OT and AI, and connectivity to more than one network where services depend on telecommunications. On coordination, they looked for permission and regular convening, safe forums for sharing failures, threat intelligence that tells operators what to act on, and work with other countries on shared capability. From government, they asked for a consolidated national risk assessment that ranks risk across sectors, socio-technical mapping of critical infrastructure, technical capability in the regulator, crisis plans tested with the people who would carry them out (including clarity on how last-resort powers would work), incident reporting obligations for the providers of AI models, narrower regulation supported by accreditation and industry peer review, and domestic investment in compute, the application layer and the pathway from research to deployment. They also cautioned against shortening incident notification windows, because accuracy in a first assessment matters more than speed, and against asking operators to do more with the same resources, which concentrates risk.

How the report uses these findings

The report draws on the interviews where participants' experience supports, develops or challenges findings from other evidence. The interviews are a source of judgement and detail from people who work with these systems.

Australia does not need to develop a national resilience framework from first principles. The CIRS provides the national policy foundation, the TISN provides an established collaboration network, and the SOCI Act provides enforceable obligations. The *Principles of Operational Technology Cyber Security* provides operational guidance that can be applied within regulated entities, while Infrastructure Australia's *Resilience Principles* provides the broader systems and community view.



Endnotes

1. Australian Signals Directorate's Australian Cyber Security Centre, Annual Cyber Threat Report 2024–25 Fact Sheet: For Critical Infrastructure (2025), https://www.cyber.gov.au/sites/default/files/2025-10/Annual%20Cyber%20Threat%20Report%202024-25%20factsheet%20for%20critical%20infrastructure.pdf, accessed 7 October 2026.
2. Australian Signals Directorate, ASD Cyber Threat Report 2022–23 (2023), https://www.cyber.gov.au/sites/default/files/2023-11/asd-cyber-threat-report-2023.pdf, accessed 7 October 2026.
3. Stephanie Crowe et al., The AI Shift in Cyber Risk: Why Leaders Must Act Now, joint statement by the leaders of the Five Eyes cyber security agencies (2026), https://www.cyber.gov.au/sites/default/files/2026-06/Five%20eyes%20cyber%20security%20agencies%20statement.pdf, accessed 7 October 2026.
4. Australian Signals Directorate's Australian Cyber Security Centre, Annual Cyber Threat Report 2024-2025 (2025), https://www.cyber.gov.au/sites/default/files/2025-10/Annual%20Cyber%20Threat%20Report%202024-25.pdf, accessed 7 October 2026.
5. Jill Slay, Independent Review of the Security of Critical Infrastructure Act 2018, final report (Department of Home Affairs, 2026), https://www.homeaffairs.gov.au/cyber-security-subsite/files/independent-review-soci-act-final-report.pdf, accessed 7 October 2026.
6. Department of Home Affairs, Streamlining and Modernising the Security of Critical Infrastructure Act 2018 (2026), https://www.homeaffairs.gov.au/how-to-engage-us-subsite/files/consultation-on-proposed-amendments-to-streamline-and-modernise-the-soci-act-2018/consultation-paper.pdf, accessed 7 October 2026.
7. Department of the Prime Minister and Cabinet (New Zealand), Enhancing the Cyber Security of New Zealand's Critical Infrastructure System: Digitally Resilient Critical Infrastructure Services to Power New Zealand's Economy and Protect Our Communities (2026), https://www.dpmc.govt.nz/sites/default/files/2026-03/nz-cyber-security-discussion-doc-feb-2026-v2.pdf, accessed 7 October 2026.
8. Security of Critical Infrastructure Legislation Amendment (Enhanced Critical Infrastructure Risk Management Program) Rules 2026 (Cth), F2026L00701, https://www.legislation.gov.au/F2026L00701/latest, accessed 7 October 2026.
9. Critical Infrastructure Security Centre, Critical Infrastructure Annual Risk Review, 3rd ed. (Department of Home Affairs, 2025), https://www.cisc.gov.au/resources-subsite/Documents/critical-infrastructure-annual-risk-review-2025.pdf, accessed 7 October 2026.
10. Security of Critical Infrastructure Act 2018 (Cth), https://www.legislation.gov.au/Series/C2018A00029, accessed 7 October 2026.
11. Emergency Management Victoria, Victoria's Critical Infrastructure All Sectors Resilience Report 2025 (2026), https://files.emv.vic.gov.au/2026-02/Victorias%20Critical%20Infrastructure%20All%20Sectors%20Resilience%20Report%202025%20V2.pdf, accessed 7 October 2026.
12. Queensland Fire and Emergency Services, Queensland Critical Infrastructure Disaster Risk Assessment (2024), https://www.disaster.qld.gov.au/__data/assets/pdf_file/0037/517996/critical-infrastructure-disaster-risk-assessment-report.pdf, accessed 7 October 2026.
13. Critical Infrastructure Security Centre, Risk Advisory for Critical Infrastructure (Department of Home Affairs, 2026), https://www.cisc.gov.au/resources/pdf-documents, accessed 7 October 2026.
14. Queensland Audit Office, Managing Third-Party Cyber Security Risks, Report 13: 2025-26 (2026), https://www.qao.qld.gov.au/sites/default/files/2026-03/Managing%20third-party%20cyber%20security%20risks%20%28Report%2013%20%E2%80%93%202025%E2%80%9326%29.pdf, accessed 7 October 2026.
15. Department of the Prime Minister and Cabinet (New Zealand), Proactive Release: Enhancing Critical Infrastructure Resilience (2023), https://www.dpmc.govt.nz/sites/default/files/2023-11/cab-23-sub-0226-enhancing-critical-infrastructure.pdf, accessed 7 October 2026.
16. Department of Home Affairs, Critical Infrastructure Resilience Plan 2023 (2023), https://www.cisc.gov.au/resources-subsite/Documents/critical-infrastructure-resilience-plan-2023.pdf, accessed 7 October 2026.
17. Huon Curtis et al., Australian Telecommunications Sector Resilience Profile: Keeping Australia Connected in an Uncertain World (ANU Tech Policy Design Centre, 2024), https://techpolicy.au/wp-content/uploads/2024/10/ANU-ATSRP-Report_2024-Final.pdf, accessed 7 October 2026.
18. Hannah Merchant, Sovereignty through Managed Dependence: Australia's Strategy for Frontier AI Access (United States Studies Centre, 2026), https://cdn.sanity.io/files/ooh1fq7e/production/ed4a6488737062dbb3d8eae238d6e57b1771781f.pdf/Sovereignty-through-managed-dependence-Australias-strategy-for-frontier-AI-access.pdf, accessed 7 October 2026.
19. Australian Cyber Security Centre, ACSC Annual Cyber Threat Report, July 2021–June 2022 (Australian Signals Directorate, 2022), https://www.cyber.gov.au/sites/default/files/2023-03/ACSC-Annual-Cyber-Threat-Report-2022_0.pdf, accessed 7 October 2026.
20. ISA Global Cybersecurity Alliance, Security of Industrial Automation and Control Systems: An Overview of ISA/IEC 62443 Standards (International Society of Automation, 2024), https://isagca.org/hubfs/2023%20ISA%20Website%20Redesigns/ISAGCA/PDFs/ISAGCA%20Quick%20Start%20Guide.pdf, accessed 7 October 2026.
21. Keith Stouffer et al., Guide to Operational Technology (OT) Security, NIST Special Publication 800-82r4, initial public draft (National Institute of Standards and Technology, 2026), https://doi.org/10.6028/NIST.SP.800-82r4.ipd, accessed 7 October 2026.
22. Rajiv Shah, Protecting Critical National Infrastructure in an Era of IT and OT Convergence, Policy Brief, Report No. 18/2019 (Australian Strategic Policy Institute, 2019), https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2019-06/Protecting%20critical%20national%20infrastructure.pdf, accessed 7 October 2026.
23. Audit Office of New South Wales, Cyber Security Insights 2025, NSW Auditor-General's Report to Parliament (2025), https://www.audit.nsw.gov.au/sites/default/files/documents/Final%20report%20-%20%20-%20Cyber%20security%20insights%202025.pdf, accessed 7 October 2026.
24. Australian Signals Directorate's Australian Cyber Security Centre, Defending against AI-Enabled Cyber Attacks: Guidance for Government, Critical Infrastructure and Large Enterprises (2026), https://www.cyber.gov.au/sites/default/files/2026-07/Defending%20against%20AI-enabled%20cyber%20attacks%20-%20Guidance%20for%20government%2C%20critical%20infrastructure%20and%20large%20enterprises.pdf, accessed 7 October 2026.
25. Department of Infrastructure, Transport, Regional Development, Communications and the Arts, Review into the Optus Outage of 8 November 2023: Final Report (2024), https://www.infrastructure.gov.au/sites/default/files/documents/review_into_the_optus_outage_of_8_november.pdf, accessed 7 October 2026.
26. Department of Home Affairs, Consultation Paper: Proposed Amendments to the Ministerial Directions Powers in Part 3 of the Security of Critical Infrastructure Act 2018 (2026), https://www.homeaffairs.gov.au/how-to-engage-us-subsite/files/consultation-on-proposed-amendments-to-ministerial-directions-powers-cirmp/public-consultation-paper-soci-act-ministerial-directions-reforms.pdf, accessed 7 October 2026.
27. Critical Infrastructure Security Centre, Trusted Information Sharing Network Framework (Department of Home Affairs, 2026), https://www.cisc.gov.au/resources-subsite/Documents/tisn-overview.pdf, accessed 7 October 2026.
28. Department of Home Affairs, Consultation on Proposed Amendments to the Ministerial Directions Powers in Part 3 of the Security of Critical Infrastructure Act 2018: Consultation and Feedback Summary (2026), https://www.homeaffairs.gov.au/how-to-engage-us-subsite/files/ministerial-directions-powers-and-exposure-draft/soci-directions-powers-reforms-consultation-and-feedback-summary.pdf, accessed 7 October 2026.
29. Cybersecurity and Infrastructure Security Agency and Australian Signals Directorate's Australian Cyber Security Centre, Principles for the Secure Integration of Artificial Intelligence in Operational Technology (2025), https://www.cyber.gov.au/sites/default/files/2025-12/principles-for-the-secure-integration-of-artificial-intelligence-in-operational-technology.pdf, accessed 7 October 2026.
30. Cyber and Infrastructure Security Centre, Artificial Intelligence in Critical Infrastructure, Factsheet for Critical Infrastructure (Department of Home Affairs, 2025), https://www.cisc.gov.au/resources-subsite/Documents/artificial-intelligence-factsheet.pdf, accessed 7 October 2026.
31. Cyber and Infrastructure Security Centre, Guidance for the Critical Infrastructure Risk Management Program (Department of Home Affairs, 2025), https://www.cisc.gov.au/resources-subsite/Documents/guidance-for-the-critical-infrastructure-risk-management-program.pdf, accessed 7 October 2026.
32. Department of Home Affairs, Regulation Impact Statement: A Risk Management Program Framework for Critical Infrastructure Assets (Office of Impact Analysis, Department of the Prime Minister and Cabinet, 2023), https://oia.pmc.gov.au/sites/default/files/posts/2023/02/Impact%20Analysis.pdf, accessed 7 October 2026.
33. Australian National Audit Office, Management of Cyber Security in the Department of Parliamentary Services, Auditor-General Report No. 38 2025-26 (2026), https://www.anao.gov.au/sites/default/files/2026-06/Auditor-General_Report_2025-26_38.pdf, accessed 7 October 2026.
34. National Cyber Security Centre (UK), Cyber Assessment Framework 4.0 (2025), https://www.ncsc.gov.uk/files/NCSC-Cyber-Assessment-Framework-4.0.pdf, accessed 7 October 2026.
35. Emergency Management Act 2013 (Vic), https://www.legislation.vic.gov.au/in-force/acts/emergency-management-act-2013, accessed 7 October 2026; Inspector-General for Emergency Management, Critical Infrastructure Resilience Implementation Progress Report 2017 (2018), https://files.igem.vic.gov.au/2021-03/Critical%20Infrastructure%20Resilience%20Implementation%20Progress%20Report%202017.PDF, accessed 7 October 2026.
36. Australian Competition and Consumer Commission, Digital Platform Services Inquiry: Final Report (2025), https://www.accc.gov.au/system/files/digital-platform-services-inquiry-final-report-march2025.pdf, accessed 7 October 2026.
37. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive), Official Journal of the European Union L 333 (2022), https://eur-lex.europa.eu/eli/dir/2022/2555/oj, accessed 7 October 2026.
38. Australian Academy of Science, Bringing Australia's Supercomputing Up to Speed (2025), https://science.org.au/sites/default/files/Event/document/bringing-australias-supercomputing-up-to-speed-fact-sheet.pdf, accessed 7 October 2026.
39. Australian Academy of Technological Sciences and Engineering, Made in Australia: Our AI Opportunity, action statement (2025), https://www.atse.org.au/media/ylsbf4m1/atse-action-statement-v2.pdf, accessed 7 October 2026.

40. Australian Academy of Technological Sciences and Engineering, Submission on Supporting the Development of Sovereign Capability in the Australian Tech Sector (2024), https://www.atse.org.au/media/efcl2t2o/sbm-2024-02-23-sovereign-capacity-in-australian-tech-sector.pdf, accessed 7 October 2026.
41. European Commission, Action Plan on Cybersecurity and Artificial Intelligence, COM(2026) 577 final (2026), https://digital-strategy.ec.europa.eu/en/library/eu-action-plan-cybersecurity-and-artificial-intelligence, accessed 20 July 2026.
42. Australian Climate Service, Australia's National Climate Risk Assessment 2025 (2025), https://www.acs.gov.au/, accessed 20 July 2026.
43. ABC News, "Global ransomware group reportedly claim cyber attack that shut down Mackay Sugar mills", 2026, accessed 11 November 2026.
44. Senate Environment and Communications References Committee, Triple Zero Service Outage (Parliament of Australia, 2026), https://parlinfo.aph.gov.au/parlInfo/download/committees/reportsen/RB000723/toc_pdf/TripleZeroserviceoutage.pdf, accessed 7 October 2026.
45. Technology Audit Partners, Findings Report on the July 8th Telstra Outage (Telstra, 2026), https://www.telstra.com.au/content/dam/tcom/dynamic-media-projects/luke-campbell/TAP-Findings-for-Telstra-Outage.pdf, accessed 7 October 2026.
46. Dragos, Inc., 2025 OT Cybersecurity Action Guide: Australia & New Zealand (2025), https://hub.dragos.com/year-in-review-action-guide-2025-anz, accessed 7 October 2026.
47. Australian Signals Directorate's Australian Cyber Security Centre, Principles of Operational Technology Cyber Security, co-sealed by Cybersecurity and Infrastructure Security Agency, National Security Agency, Federal Bureau of Investigation and international partners (2024), https://www.cyber.gov.au/sites/default/files/2025-03/Principles%20of%20operational%20technology%20cybersecurity%20%28October%202024%29.pdf, accessed 7 October 2026.
48. Emergency Management Victoria, Victoria's Critical Infrastructure All Sectors Resilience Report 2024 (2025), https://files.emv.vic.gov.au/2025-11/SIGNED_EMV%20Victorias%20Critical%20Infrastructure%20All%20Sectors%20Resilience%20Report%202024.pdf, accessed 7 October 2026.
49. Department of Home Affairs, Critical Infrastructure Resilience Strategy (2023), https://www.cisc.gov.au/resources-subsite/Documents/critical-infrastructure-resilience-strategy-2023.pdf, accessed 7 October 2026.
50. Infrastructure Australia, Resilience Principles: Infrastructure Australia's Approach to Resilience (2022), https://www.infrastructureaustralia.gov.au/sites/default/files/2022-06/Resilience%20Principles%20-%20Infrastructure%20Australia%27s%20approach%20to%20resilience.pdf, accessed 7 October 2026.
51. Cyber and Infrastructure Security Centre, Critical Infrastructure Risk Management Program, factsheet (Department of Home Affairs, 2025), https://www.cisc.gov.au/resources-subsite/Documents/cisc-factsheet-risk-management-program.pdf, accessed 7 October 2026.
52. Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements," proposed rule, Federal Register 89, no. 66 (2024): 23644, https://www.govinfo.gov/content/pkg/FR-2024-04-04/pdf/2024-06526.pdf, accessed 7 October 2026.
53. Australian Signals Directorate, Annual Cyber Threat Report 2023-2024 (2024), https://www.cyber.gov.au/sites/default/files/2024-11/asd-cyber-threat-report-2024.pdf, accessed 7 October 2026.
54. OpenAI, OpenAI - Hugging Face Incident Technical Report (2026), https://cdn.openai.com/pdf/67869394-cb91-4c12-888c-5cbd85c7814c/OpenAI-Hugging-Face%20Incident-Technical-Report.pdf, accessed 7October 2026.
55. Anthropic, "Improving Our Alignment and Security Efforts," 2026, https://www.anthropic.com/news/improving-alignment-security-efforts, accessed 7 October 2026.
56. Department of Home Affairs, Consultation Paper: Proposed Amendments to Enhance the Critical Infrastructure Risk Management Program Rules (CIRMP Rules) (2025), https://www.homeaffairs.gov.au/how-to-engage-us-subsite/files/consultation-on-enhancements-to-cirmp-rules/consultation-paper-proposed-amendments-enhance-cirmp.pdf, accessed 7 October 2026.
57. Yanfang Wu et al., "Attack-Defense Game of Interdependent Infrastructure Systems Considering Cascading Failures," Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability 239, no. 6 (2025): 1281-1295, https://doi.org/10.1177/1748006X251336007, accessed 7 October 2026.
58. Su Liu et al., "Cascading Failure in Multiple Critical Infrastructure Interdependent Networks of Syncretic Railway System," IEEE Transactions on Intelligent Transportation Systems 23, no. 6 (2022): 5740-5753, https://doi.org/10.1109/TITS.2021.3057404, accessed 7 October 2026.
59. Gian Paolo Cimellaro, Alessandro Cardoni, and Andrei Reinhorn, "Modelling Infrastructure Interdependencies and Cascading Effects Using Temporal Networks," Resilient Cities and Structures 3, no. 3 (2024): 28-42, https://doi.org/10.1016/j.rcns.2024.05.002, accessed 7 October 2026.
60. Ryan Hoff et al., "Cascading Failure Propagation and Perfect Storms in Interdependent Infrastructures," ASCE OPEN: Multidisciplinary Journal of Civil Engineering 3, no. 1 (2025): 04025001, https://doi.org/10.1061/AOMJAH.AOENG-0045, accessed 7 October 2026.
61. Cong Lu et al., "Optimizing Urban Infrastructure Resilience: Analyzing Cascading Failures and Critical Node Dependencies through Multilayer Network Models," Journal of Safety Science and Resilience 7 (2026): 100245, https://doi.org/10.1016/j.jnlssr.2025.100245, accessed 7 October 2026.
62. Australian Prudential Regulation Authority, Prudential Practice Guide CPG 230 Operational Risk Management (2026), https://www.apra.gov.au/system/files/2026-05/Prudential%20Practice%20Guide%20CPG%20230%20-%20Operational%20Risk%20Management%20-%20clean.pdf, accessed 7 October 2026.
63. Financial Stability Board, Enhancing Third-Party Risk Management and Oversight: A Toolkit for Financial Institutions and Financial Authorities (2023), https://www.fsb.org/uploads/P041223-1.pdf, accessed 7 October 2026.
64. Prashant Tyagi, "Convergence of IT and OT: Cybersecurity Related Challenges and Best Practices," International Journal of Computer Trends and Technology 69, no. 2 (2021): 85-92, https://doi.org/10.14445/22312803/IJCTT-V69I2P113, accessed 7 October 2026.
65. Yassine Maleh, "IT/OT Convergence and Cyber Security," Computer Fraud & Security, no. 12 (2021): 13-16, https://doi.org/10.1016/S1361-3723(21)00129-9, accessed 7 October 2026.
66. ISA Global Cybersecurity Alliance, Applying ISO/IEC 27001, ISO/IEC 27002 and the ISA/IEC 62443 Series for Operational Technology Environments (2025), https://www.isa.org/getmedia/12ce5956-3047-4820-899c-5158722039d9/ISAGCA_Applying-ISO-IEC-27001-2-and-the-62443-Series_White-Paper_2025.pdf, accessed 7 October 2026.
67. Banking, Insurance, Life Insurance, Health Insurance and Superannuation (prudential standard) determination No. 1 of 2026 (Cth), F2026L00475, schedule (Prudential Standard CPS 230 Operational Risk Management), https://www.legislation.gov.au/F2026L00475, accessed 7 October 2026.
68. Colin Topping et al., "Beware Suppliers Bearing Gifts! Analysing Coverage of Supply Chain Cyber Security in Critical National Infrastructure Sectorial and Cross-Sectorial Frameworks," Computers & Security 108 (2021): 102324, https://doi.org/10.1016/j.cose.2021.102324, accessed 7 October 2026.
69. Mari Aarland and Terje Gjøsæter, "Digital Supply Chain Vulnerabilities in Critical Infrastructure: A Systematic Literature Review on Cybersecurity in the Energy Sector," in Proceedings of the 8th International Conference on Information Systems Security and Privacy (ICISSP 2022) (SciTePress, 2022), 326-333, https://doi.org/10.5220/0010803800003120, accessed 7 October 2026.
70. Office of the Auditor General Western Australia, Cyber Security in Local Government, Report 9: 2021-22 (2021), https://audit.wa.gov.au/wp-content/uploads/2021/11/Report-9_Cyber-Security-in-Local-Government.pdf, accessed 7 October 2026.
71. Queensland Audit Office, Responding to and Recovering from Cyber Attacks, Report 12: 2023-24 (2024), https://www.qao.qld.gov.au/sites/default/files/2024-06/Responding%20to%20and%20recovering%20from%20cyber%20attacks%20%28Report%2012%20%E2%80%93%202023%E2%80%9324%29_0.pdf, accessed 7 October 2026.
72. Victorian Auditor-General's Office, Security of Water Infrastructure Control Systems, PP No. 28, Session 2018-19(2019),https://www.audit.vic.gov.au/sites/default/files/2019-05/29052019-Water-Control-Systems.pdf, accessed 7 October 2026.
73. Tony Burke, "Consultation Opens on Critical Infrastructure Reforms," media release, 2026, https://minister.homeaffairs.gov.au/TonyBurke/Pages/consultation-opens-on-critical-infrastructure-reforms.aspx,accessed 7 October 2026.
74. Australian National Audit Office, Defence's Management of ICT Systems Security Authorisations, Auditor-General Report No. 2 2024-25 (2024), https://www.anao.gov.au/sites/default/files/2024-09/Auditor-General_Report_2024-25_2.pdf, accessed 7 October 2026.
75. Audit Office of New South Wales, Cyber Security in Local Health Districts, NSW Auditor-General's Report to Parliament (2025), https://www.audit.nsw.gov.au/sites/default/files/documents/Final%20report%20-%20Cyber%20security%20in%20LHDs.pdf, accessed 7 October 2026.
76. NSW Department of Justice, Office of Emergency Management, NSW Critical Infrastructure Resilience Strategy 2018 (2018), https://data.nsw.gov.au/data/dataset/3-19084-nsw-critical-infrastructure-resilience-strategy-, accessed 7 October 2026.
77. Donald Azuatalam et al., "Measuring Electricity Infrastructure Resilience: A Comparative Review of Reliability and Resilience Metrics" (working paper, SSRN, 2026), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=6904058, accessed 7 October 2026.



Australian Academy of Technological Sciences & Engineering

ACKNOWLEDGEMENT OF COUNTRY

We acknowledge Traditional Owners of Country across Australia and recognise their continuing connection to land, water and community. We pay respect to Aboriginal and Torres Strait Islander culture, and Elders past and present.

atse.org.au

261112