Australian Government
Department of Home Affairs

Security of Critical Infrastructure

Streamlining and Modernising the *Security of Critical Infrastructure Act 2018*

Contact us
Enquiries regarding the licence and any use of this document are welcome at:

Critical Infrastructure Security Policy Branch
Department of Home Affairs
PO Box 25
BELCONNEN ACT 2616

Table of Contents

Introduction

Australia's critical infrastructure underpins the essential services on which all Australians depend. Its security and resilience are fundamental to national security, public safety, social wellbeing, productivity and economic stability. Secure and reliable infrastructure helps businesses, households and governments operate with confidence, and reduces the consequences of disruptive shocks.

The *Security of Critical Infrastructure Act 2018* (SOCI Act) has made an important contribution to Australia's critical infrastructure security framework. It has improved visibility of critical assets, lifted executive and board-level attention to infrastructure risk, supported more consistent incident reporting, and created a common language for government and industry to discuss cyber, physical, personnel, supply chain and operational resilience risks.

Practical experience has shown that parts of the SOCI framework are too complex, duplicative or difficult to apply in contemporary operating environments. Entities can face overlapping obligations under SOCI and other Commonwealth, State, Territory and sector-specific frameworks. Some asset definitions no longer align with modern service delivery, dependency, ownership and control models. Current compliance and assurance settings also do not always give entities, boards or Government a clear view of whether risk management arrangements are effective in practice.

The proposed reforms have three linked objectives. First, they would reduce unnecessary duplication, complexity and uncertainty. Secondly, they would modernise and refine sector and asset coverage, so the framework continues to address nationally significant risks. Thirdly, they would clarify the expectations, assurance mechanisms and governance settings needed to assess whether security and resilience outcomes are being achieved.

Taken together, the proposed reforms would refine Australia's critical infrastructure regulatory framework by improving workability, addressing known gaps, and supporting more effective security and resilience outcomes across critical infrastructure sectors.

A central purpose of the reforms is to make the framework clearer for regulated entities. Clearer statutory concepts, guidance and assurance arrangements will help entities understand what Government expects, when obligations apply, who is responsible and how compliance can be demonstrated. They will also support a more mature approach to assessing whether risk management arrangements are operating effectively.

The Government recognises that regulation must be proportionate and workable. Poorly calibrated requirements can impose unnecessary cost, slow investment and divert resources from substantive risk reduction. The proposals in this paper seek to focus regulatory effort on material risk, recognise equivalent outcomes where they already exist, preserve asset visibility and targeted intervention powers where necessary, and provide clearer pathways for industry and Government to manage critical infrastructure security together.

Unless otherwise specified, references in this paper to "the Department", "the Secretary" and "the Minister" are to the Department of Home Affairs, the Secretary of the Department of Home Affairs and the Minister for Home Affairs, respectively.

Scope of this consultation

This paper seeks views on proposed amendments to the SOCI Act. The main question for stakeholders is whether the proposed reform direction is clear, proportionate, and capable of reducing duplication, refining coverage and supporting assurance of effective security and resilience outcomes.

The SOCI framework identifies critical infrastructure through a layered legislative structure. At the broadest level, the Act identifies sectors of the Australian economy that are relevant to critical infrastructure regulation. Within those sectors, the Act identifies classes of assets that are capable of being critical to the social or economic stability of Australia or its people, the defence of Australia, or national security. The *Security of Critical Infrastructure (Definitions) Rules* provide the more detailed prescription needed to determine which assets within those Act-level classes are critical for the purposes of the framework.

This staged design is important for understanding the scope of this consultation. In many cases, the proposed amendments in this paper would establish or refine the Act-level asset class. They would not settle the detailed thresholds, technical boundaries, exclusions or operational settings that determine the final regulated cohort. Those matters would be developed through subsequent consultation on amendments to the Definitions Rules and, where relevant, other subordinate instruments.

For example, the SOCI Act currently identifies certain electricity generation stations as a class of critical electricity asset. It provides that an electricity generation station is a critical electricity asset if it is critical to ensuring the security and reliability of electricity networks or electricity systems in a State or Territory, in accordance with requirements prescribed by the Rules. The Definitions Rules then narrow that class by reference to matters such as system restart ancillary service arrangements, installed capacity and connection to a wholesale electricity market. In this way, the Act identifies the relevant asset class, and the Rules provide the thresholds and technical boundaries that determine which assets within that class are captured.

The same approach is intended for many of the proposed measures. The question for this consultation is whether the proposed Act-level asset classes properly respond to the risks, regulatory gaps and policy problems identified for each measure. Stakeholders are invited to comment on whether those classes are appropriately framed, whether they capture the right kinds of assets, whether they are too broad or too narrow, and whether any safeguards, exclusions or alternative approaches should be considered.

The Department recognises that stakeholders may also have views on the detailed requirements that should apply at the Rules level. Those views are welcome where they assist in testing the workability and proportionality of the proposed Act-level model. Detailed Rules-level thresholds, technical boundaries, exclusions and operational settings will be subject to further consultation. That later process will be used to ensure that only assets that are truly critical are captured.

For each measure, this paper sets out a proposed model for consultation. Each model reflects the Department's current policy direction and is intended to give stakeholders a clear basis for comment.

The Department is also undertaking comprehensive regulatory Impact Analysis in parallel with this consultation process. Each measure in this paper identifies, where presently available, the Department's current understanding of likely affected cohorts, impact pathways, cost drivers and implementation issues. Where the affected population or regulatory burden depends on Rules-level thresholds, exclusions, equivalent-framework recognition or transition settings, the final assessment will necessarily depend on the detailed settings settled through subsequent design work. The Department will use consultation evidence to inform the final Impact Analysis that will accompany the Government's final policy decision.

Have your say

We encourage you to respond to the consultation questions in this paper. You are welcome to answer only those questions that are relevant to you or your organisation.

The proposals outlined in this paper are for consultation and are not yet law. Feedback received through this process will inform decisions on the design of the legislative package, subordinate instruments, implementation sequencing and supporting guidance.

The consultation period closes at midnight (AEST) on 31 July 2026.

We will publish written submissions unless otherwise advised. We may redact parts of published submissions that contain commercially sensitive information, or information that is protected under Part 4 of the SOCI Act. We will treat any personal information shared through the consultation process in accordance with the *Privacy Act 1988* (Cth).

Independent Review of the SOCI Act

Dr Jill Slay AM conducted an Independent Review of the SOCI Act between November 2025 and January 2026. The final report was tabled in Parliament on 24 March 2026. The Review drew on written submissions, survey responses, roundtables, Commonwealth agency input and international legislative comparison. It examined whether the Act is achieving its intended objectives, functioning as intended, or producing any unintended consequences.

Key findings

The Review found that the SOCI Act has made an important contribution to Australia's critical infrastructure security framework. Stakeholders acknowledged that it has increased executive and board-level awareness of infrastructure vulnerabilities, established baseline governance and accountability structures, improved asset visibility and incident reporting, and created a common language for discussing critical infrastructure risk. At the same time, stakeholders consistently identified complexity, duplication and operational difficulty as barriers to the framework working effectively in practice.

The Review's overarching conclusion was that the SOCI Act requires legislative change to reduce complexity and confusion, simplify its operation, and make the framework more agile and responsive to emerging threats. It also concluded that the framework should move toward a more outcome-driven model focused on measurable improvements in security risk management.

The Review identified five main themes requiring reform.

Theme	Key findings
Complexity and clarity	Stakeholders identified complexity, confusion and duplication as central concerns. Around 70 per cent of recorded sentiment described the SOCI framework in those terms. More than half of respondents said obligations were unclear, and a large majority said definitions were problematic.
Regulatory duplication	Regulatory overlap emerged as a major issue across surveys, submissions and roundtables. In the survey, 55.6 per cent of respondents reported overlap with other frameworks. The Review identified duplication with APRA CPS 230 and CPS 234, the Privacy Act, Defence Industry Security Program (DISP), Protective Security Policy Framework (PSPF), and State-level frameworks as prominent concerns.
Enforcement posture	The Review found that stakeholders considered the current enforcement posture too weak to support effective accountability. Stakeholders expressed concern that the framework had become too focused on administration and documentation, and not sufficiently focused on effective risk management, testing, remediation and visible accountability. The Review linked this perception to weaker board engagement and reduced confidence that the framework is driving genuine security uplift.
Coverage gaps, asset definitions, and emerging threats	The Review found that the current framework is not sufficiently agile or calibrated for emerging technologies, contemporary operating models, or critical functions that do not fit existing sector and asset definitions. It supported further consideration of potential coverage gaps relating to artificial intelligence infrastructure and services, hyperscale cloud, content delivery networks, space and satellite dependencies, drones, assets under

Theme	Key findings
	construction, and energy-transition risks, including inverter original equipment manufacturers, aggregators and virtual power plant operators. The Review also identified definitional issues in the higher education and research sector, and the health care and medical sector. These included research security and foreign interference risks, the treatment of research institutions beyond universities, Defence-funded research, critical health care assets and medical supply-chain dependencies. It further concluded that the framework remains too focused on cyber security, and should better address physical security, personnel security and all-hazards supply-chain risks.
Assurance	The Review found that self-attestation by boards remains a weak assurance mechanism on its own. There was strong support for introducing appropriately qualified external assurance, and more generally for moving from procedural, document-based compliance toward effectiveness-based assurance that better tests whether security outcomes are being achieved in practice.

Government response to the Independent Review

The Government has accepted all six recommendations of the Review in principle. The response will be delivered through a staged program of legislative reform, guidance and broader implementation work. Some recommendations will be implemented through more than one amendment, consultation process or implementation activity. This reflects the Review's finding that the SOCI framework needs immediate workability improvements as well as a longer-term program of simplification and rationalisation.

The immediate legislative program has two linked stages.

Tranche 1 has been advanced separately through:

- amendments to enhance the *Critical Infrastructure Risk Management Program Rules* (CIRMP Rules), including changes to specified all-hazards, cyber, supply chain, physical and personnel-security settings for specified high-risk asset classes; and

- consultation on proposed amendments to the Ministerial directions framework in Part 3 of the SOCI Act, including amendments to the existing general direction power in section 32 and new powers relating to governance-related conditions, high-risk vendors, delayed continuous disclosure, and civil penalties for non-compliance with directions.

These measures address immediate risk management, prevention and intervention settings. They are intended to strengthen entity-led risk management and give Government targeted and proportionate tools for serious national security risks that cannot be adequately addressed through ordinary engagement or existing controls.

Tranche 2, which is the focus of this paper, addresses broader concerns relating to the structure and operation of the SOCI framework. It proposes reforms to reduce duplication, refine and modernise sector and asset coverage, improve reporting architecture, strengthen governance and assurance, clarify operational-control settings, and better support contemporary ownership, service and dependency models.

The two tranches are complementary parts of a single reform program. Tranche 1 addresses immediate risk and intervention settings; Tranche 2 improves the underlying architecture so the Act is clearer, more targeted, easier to operate and better able to support assurance of practical security and resilience outcomes.

The Government recognises Recommendation 6 of the Review, which called for work toward simplification and rationalisation of the SOCI Act framework and, over time, a simpler principles-based model supported by Rules and thematic guidance. The Government is committed to that goal. Many Tranche 1 and Tranche 2 measures advance that work within the current statutory framework by clarifying boundaries, creating more coherent mechanisms for managing overlap, and strengthening supporting assurance and governance settings.

At the same time, the present threat environment and the scale of national security risk also require priority action to close known gaps in our laws. The Review identified significant concerns relating to duplication, weak enforcement, emerging technologies, vendor and supply chain risks, energy transition vulnerabilities, gaps in sector coverage, and the limited availability of timely intervention tools. The Government will continue longer-term simplification while progressing reforms that are presently needed to protect Australia's security, resilience, safety and prosperity, and the communities that depend on essential services.

This approach recognises that unmanaged vulnerabilities in critical infrastructure can directly affect economic resilience and productivity. Disruption to communications, data, energy, freight, health, transport, research or other critical infrastructure can impose direct costs on businesses and households, interrupt supply chains, reduce confidence and delay investment. A clearer and more proportionate SOCI framework supports productivity by reducing uncertainty, focusing regulatory effort on material risk, and improving the resilience of the infrastructure on which a modern economy depends.

The Government also accepts the Review's emphasis on reducing unnecessary regulatory burden. Recommendation 1 called for the removal of all possible Commonwealth regulatory duplication from the SOCI Act. That objective is reflected through the proposed exemptions framework, which would provide a more coherent basis for targeted relief where another Commonwealth, State or Territory law, or another recognised framework, already imposes substantially equivalent requirements. The purpose is to reduce overlap while preserving any SOCI settings still needed for visibility, assurance, notification or coordinated risk management.

Because the interaction between SOCI and other frameworks is often sector-specific and operationally complex, effective anti-duplication reform will require close engagement with industry and other regulators. The Government will work closely with industry to map areas of overlap, identify where duplication arises in practice, and develop solutions that reduce burden while maintaining substantive security and resilience outcomes. That work will continue through this consultation process and through subsequent design and implementation work.

Taken together, Tranche 1, Tranche 2 and this future workstream are intended to deliver a coherent and manageable staged program of reform. The immediate objective is to close known gaps, improve operability and reduce duplication within the existing framework. The longer-term objective is to continue simplifying and rationalising the SOCI framework so that it remains capable of supporting effective security and resilience outcomes over time.

Appendix A provides a consolidated mapping of the Review's recommendations to the Government's response pathway.

Summary table of proposed reforms

The table below provides a high-level guide to the proposed reforms and the main issues on which Government is seeking views. Detailed policy design, legal effect, implementation pathways and preliminary impact analysis are set out in the relevant measure sections. For measures that may newly capture entities, the final affected population will depend on Rules-level thresholds, exclusions, equivalent-framework recognition and transition settings developed following consultation.

#	Measure	Proposed model for consultation	Why we are consulting
Part A – Reducing complexity, duplication and uncertainty			
1.	Exemptions framework	Establish a clearer exemptions framework to provide targeted relief from specified SOCI obligations where another law or recognised framework delivers substantially equivalent or stronger outcomes. Relief could be full, partial, conditional, time-limited or subject to review.	The current exemptions provisions in the Act are fragmented and can produce all-or-nothing outcomes. A clearer framework is needed to provide targeted relief where SOCI obligations duplicate equivalent frameworks, including where no practical relief mechanism currently exists.
2.	Register of Critical Infrastructure Assets	Restructure Part 2 so the Act sets broad categories of registrable information, and the Rules prescribe the detailed information items within those categories, supported by a simpler change-notification model.	The current Register provisions are too rigid and prescriptive. A clearer Act, Rules and form architecture would make registration obligations easier for entities to understand and comply with, and simpler for Government to maintain over time.
3.	Annual reporting simplification	Replace hard-coded annual reporting content with a simpler obligation to give an annual compliance report in an approved form. Reporting questions would be published in advance and could be tailored by entity, asset class or obligation type.	The current reporting model fixes too much content in the Act. A more adaptable model would make annual reporting more proportionate, predictable and useful.
4.	Part 2D notification clarification	Clarify that the Secretary's notice under Part 2D is a point-in-time assessment based on the information then available. The notice would also make clear that later or materially different changes may require further notification.	Telecommunications projects and service arrangements can evolve after an initial notification. The reform would give responsible entities clearer guidance on the legal effect of a notice and the continuing notification obligation, reducing uncertainty about whether later changes must be notified.

5.	**Cyber security incident definition involving automated systems, software agents and AI**	Refine the Act-wide definition of "cyber security incident" so it operates clearly where automation, software agents or AI-enabled tools affect the mechanism, attribution or operation of a cyber incident. The cyber security character of the incident, and the existing Part 2B impact thresholds for reportable incidents, would be preserved.	The current definition relies on concepts of unauthorised access, modification or impairment. The reform would clarify how those concepts apply where serious cyber incidents are caused by, or occur through, automated systems, while preserving the separate thresholds and safeguards that apply where the defined term is used in Part 2B, Part 2C and Part 3A.
6.	**Systems of National Significance**	Simplify the SoNS framework so designation has clearer practical consequences for the declared asset. The model would replace incident response planning with asset-specific resilience planning, retain cyber security exercises, make vulnerability assessments discretionary and all-hazards, repeal the System Information Enhanced Cyber Security Obligation (ECSO), and recognise equivalent arrangements.	The current SoNS framework is procedurally complex and can be slow to deliver practical uplift after designation. A simpler model would reduce duplication and focus enhanced obligations on preparedness, continuity, recovery and restoration for nationally significant assets.
7.	**Subsea telecommunications cables and associated infrastructure**	Refine the critical telecommunications asset framework for nationally significant submarine cable systems, including shore-end, landing, terminal, power and network-management components, distributed responsible entities, and material cable interests such indefeasible rights of use (IRUs) or consortium rights.	Current settings do not align well with contemporary cable ownership, operation and interest-holder models. The reform would clarify asset boundaries, responsible entity identification and the treatment of material cable interests. This would promote greater certainty about the scope of regulated infrastructure and the entity responsible for each relevant component or function.
8.	**Data storage or processing**	Replace the current customer-driven capture model with clearer operator-facing pathways. The model would cover significant data-centre facilities, larger service-layer providers, certified hosting providers and a limited reserve designation pathway for exceptional government-dependent cases.	Current capture depends too heavily on customer identity, data characterisation and customer notification. Operator-facing pathways would make the framework more predictable and self-assessable.

Part B – Modernising and refining sector and asset coverage			
9.	**Space technology**	Establish four space technology asset classes: ground segment infrastructure, positioning, navigation and timing (PNT) support infrastructure, earth observation data infrastructure and space situational awareness infrastructure. The Act would set the asset-class categories, with operative thresholds, specified assets, requirements and exclusions developed through later Rules consultation.	The space technology sector is listed in the Act but has no operative asset classes. The reform would give effect to the sector through bounded ground-based and associated terrestrial categories, using objective Rules-level thresholds.
10.	**Health care and medical**	Apply risk-management obligations more consistently to critical hospitals, and create new asset classes for concentrated and systemically significant blood supply, pathology, and high-containment or specialised laboratory functions.	The current framework reaches only part of the health sector's most significant infrastructure. The reform would focus on concentrated and systemically significant functions where disruption, compromise or misuse could have broader health-system, public health, biosecurity or national security consequences.
11.	**Distributed energy resources**	Update the electricity framework so it can address electricity storage, DER portfolios, controllable demand, aggregation, orchestration and dispatch arrangements. Rules-level thresholds would be developed using metrics such as registered capacity, dispatchable capacity, aggregated controllable capacity, market participation, number of controlled devices, and common operational or dispatch control.	The current framework was built around centralised, site-based assets. It does not deal clearly with storage, virtual power plants, software-enabled orchestration or coordinated portfolios that may have system effects comparable to traditional electricity assets.
12.	**Offshore electricity assets**	Disapply the geographic limitation for critical electricity assets located in Commonwealth offshore areas. Offshore assets would still need to meet the ordinary critical electricity asset definition and Rules thresholds before SOCI obligations apply.	Current location settings may exclude offshore electricity infrastructure beyond the territorial sea even where Australia regulates the project and the asset otherwise meets critical electricity thresholds.
13.	**Critical freight**	Broaden the freight framework to cover nationally significant nodes, interfaces, distribution points, logistics platforms and discrete chokepoints where disruption could affect supply	The current framework is narrow, geographically constrained and difficult to apply to modern freight dependencies. It can miss intrastate nodes, chokepoints, logistics systems and business-controlled capabilities

		chains beyond a single site or operator. Clarify that the asset of a critical freight service business is its own systems, facilities and operational capabilities. The Department is also seeking views on whether large-scale connected transport systems should be capable of capture where they materially affect freight or broader transport operations.	that are important to national supply-chain resilience. Clarifying the freight-services asset boundary would also help businesses distinguish assets they can manage from public infrastructure they merely use.
14.	**Higher education and research**	Replace the critical education asset class with a critical research asset class focused on organised research functions. Capture would require an organised research function, a prescribed sensitive research field, a prescribed national security nexus pathway and an identifiable responsible entity.	The current definition is limited to university-owned or university-operated assets and depends on a "program of research" that is "critical to" another sector, defence or national security. That model does not align well with sustained research functions, secure data environments, collaborative structures or equivalent sensitive research outside universities.
Part C – Governance, Assurance and Accountability			
15.	**CIRMP governance and assurance**	Clarify CIRMP governance, review and currency obligations, remove current admissibility restrictions for annual compliance reports, and introduce proportionate independent assurance of CIRMP design, implementation and effectiveness. The assurance model would be risk-calibrated, with internal assurance potentially available for lower-risk entities where independence and capability requirements are met.	The current framework relies heavily on self-attestation and imprecise review obligations. The reform would give entities, boards and regulators better evidence that CIRMPs are current, implemented and effective.
16.	**Graduated civil penalty settings**	Increase the maximum penalty for preventive and assurance duties from 200 to 500 penalty units. Lower-tier administrative and visibility obligations, and higher-tier direction and telecommunications obligations, would remain at their existing or separately proposed settings.	Selected risk management and assurance duties sit at the centre of the SOCI framework. A higher middle-tier maximum would improve deterrence and preserve the Act's graduated penalty structure.
17.	**Operations, maintenance, and**	Introduce a relevant operator concept for entities with material practical control over an asset or critical function. Relevant operators would be subject to	Critical operational functions are often performed by outsourced operators, MSPs, OEMs, platform administrators or subcontractors. The reform would

	managed service providers	targeted registration, limited direct duties to cooperate, notify and avoid materially compromising the asset, and direct enforcement of those duties.	preserve the responsible entity model and address operational-control risks that sit outside current ownership and direct-interest concepts.
18.	**Corporate group cooperation**	Create a limited cooperation duty for connected corporate-group entities where the responsible entity materially depends on them for CIRMP compliance. The duty would require reasonable cooperation, assistance and notification of material events, while the responsible entity would remain primarily responsible for CIRMP compliance.	Security-critical functions may sit with a parent company, shared services entity or another related body corporate. A limited cooperation duty would help responsible entities comply where key cyber, personnel, supply-chain or physical security functions sit elsewhere in the group.
19.	**Supply chain cyber security**	Clarify CIRMP expectations for cyber security assurance of major suppliers. The model would cover supplier assessment, contractual or equivalent measures, recognised certification or accreditation, documented exceptions for constrained supply chains, and material sub-tier risks considered through the direct major supplier assessment.	Supplier cyber security is part of the asset's risk picture. The reform would help responsible entities assess and manage cyber risks from major suppliers in a practical and proportionate way, and reduce duplicative assurance where recognised accreditation is relevant and properly scoped.
20.	**Specified risk information**	Create a targeted mechanism for the Secretary to specify published risk, hazard, standards or guidance material that responsible entities must consider through CIRMP processes. Entities would assess relevance, document their response and decide whether any CIRMP, control or governance update is needed.	Relevant risk information may sit outside formal risk-management decision-making. The reform would require documented consideration of specific material identified through a statutory notice process, without turning that material into a binding technical standard.
21.	**Critical workers and critical components**	Replace the current critical worker definition with a clearer access-based and authority-based model, supported by a refined critical component concept. The Rules could create categories of critical worker and apply proportionate checking, monitoring, training, supervision or access-control requirements.	The current definition is difficult to apply consistently and relies too heavily on broad responsible-entity assessments. The reform would make the framework clearer for direct employees, contractors and relevant third-party personnel whose role, access or authority creates personnel-security risk.

Part A – Reducing Complexity, Duplication and Uncertainty

A.1 – Reducing duplication

Measure 1 – Exemptions Framework

The problem

The SOCI Act currently manages duplication through a patchwork of obligation-specific exemption mechanisms. Those mechanisms are limited in scope, operate differently across different Parts of the Act, and do not provide a consistent basis for managing overlap across the framework. In some Parts of the Act, there is no practical exemption mechanism at all. This means the availability and scope of relief can depend on the Part of the Act that applies, rather than on a clear principle about when equivalent regulation should reduce or modify SOCI requirements.

The current CIRMP exemption mechanism also lacks precision. It effectively operates on an all-or-nothing basis and does not allow relief to be calibrated to the requirements that are actually duplicative. It cannot readily preserve residual obligations, such as reporting, assurance, notification or cooperation requirements, where those obligations are still needed even if another regime addresses the main risk-management requirement.

The result can be unnecessary duplication where another law or recognised framework already manages the same risk to an equivalent or stronger standard. It can also leave entities uncertain about which SOCI obligations continue to apply when they operate across multiple regulatory regimes.

> **Proposed model for consultation:** The Act would establish a single, consolidated exemptions framework that could apply across a range of specified SOCI obligations. Relief would be available where another Commonwealth, State or Territory law, or another recognised enforceable framework, delivers substantially equivalent or stronger outcomes for the same asset, entity, function or risk.
>
> Exemptions could be limited, conditional and subject to review. This would allow SOCI requirements to continue where they are still needed for visibility, notification, assurance, coordination or national security risk management.
>
> The framework would include safeguards to ensure exemptions remain targeted and current. These could include criteria for assessing equivalence, conditions on exemptions, review arrangements, variation and revocation powers, periodic reassessment where the recognised framework or risk environment changes, and publication requirements for exemption decisions to ensure transparency.

Example – transport security: The proposed exemptions framework could apply where a critical infrastructure asset is also regulated under transport security legislation, including the maritime transport and offshore facilities security framework. Operators may already be required to prepare and maintain

security plans, manage access and security zones, conduct exercises, report incidents and engage with Government under that framework.

The proposed exemptions framework would allow that overlap to be assessed in a targeted way. Where a transport security obligation delivers substantially equivalent or stronger outcomes for the same asset, function or risk, relief could be provided from the relevant SOCI requirement. For example, an existing approved transport security plan or exercise process could be recognised for specified physical security or incident management requirements.

Relief may be limited or conditional. SOCI obligations could continue to apply where they are needed for matters not adequately addressed by the transport security framework, including cyber security, supply-chain risk, systems and dependency visibility, annual reporting, assurance, incident notification, coordination or national security risk management. This would avoid duplicative planning or reporting while preserving the parts of the SOCI framework that remain necessary to ensure the continued security and resilience of critical infrastructure.

Key design elements

Element	Description
General framework across specified obligations	Exemptions would operate across specified SOCI obligations through a single framework that could replace separate, obligation-specific exemption mechanisms where a common approach is appropriate.
Equivalence threshold	Relief would only be available where another Commonwealth, State or Territory law, or another recognised enforceable framework imposes requirements that are substantially equivalent to, or more stringent than, the relevant SOCI obligation.
Obligation-specific relief	The framework would allow targeted exemption from specified obligations, or from obligations as they apply in specified circumstances, avoiding an all-or-nothing outcome.
Conditional exemptions	Exemptions could be made subject to conditions so that residual reporting, assurance, notification or cooperation requirements can be preserved.
Individual and class-based operation	The framework would support both entity-specific and class-based relief, so it can address tailored overlap scenarios and broader categories of duplication across a sector or framework.
What is not changing	The reform would not remove core SOCI controls where they remain necessary. It is intended to manage duplication more precisely while preserving substantive security outcomes and retaining any residual SOCI requirements needed for visibility, assurance, notification, coordination or national security risk management.

Preliminary Impact Analysis

This measure is deregulatory in intent. It would allow relief to be provided from SOCI obligations that duplicate substantially equivalent requirements under another Commonwealth, State, Territory or recognised enforceable framework. The benefit would accrue to the existing regulated base, particularly entities already subject to sector regulation, such as prudentially regulated financial entities, energy market participants and telecommunications carriers.

he associated costs would depend on how relief is initiated. Where an entity seeks an exemption, costs are expected to be one-off and would primarily involve preparing an equivalence case and supporting evidence. Where the Commonwealth initiates an exemption, including a class exemption, affected entities may not need to prepare an application. Their costs would instead be limited to familiarisation, confirming whether the exemption applies to their asset or obligation, updating internal compliance processes, and meeting any conditions attached to the exemption.

The measure is not expected to increase ongoing compliance cost and may reduce it where duplication is removed. It is therefore not expected to adversely affect competition, innovation or market entry. The practical reach of the measure would depend on which frameworks are recognised as substantially equivalent and which SOCI obligations create the most material duplication in practice.

Consultation questions

1. Does the proposed obligation-specific exemption model provide a workable way to reduce duplication while preserving residual SOCI visibility, notification and assurance requirements?
2. What criteria should be used to assess whether another regime is substantially equivalent, particularly where the two frameworks use different terminology or structure but are directed to similar outcomes?
3. What SOCI obligations should be capable of full relief, partial relief or conditional relief?
4. What SOCI obligations should remain, even where another framework is recognised as substantially equivalent?
5. What safeguards should apply to class exemptions, including review, conditions, variation, revocation, publication and reporting?
6. Which SOCI obligations create the most material duplication or regulatory cost in practice, and which existing frameworks should be assessed first for equivalence?

A.2 – Simplifying administration, reporting and notification

Measure 2 – Register of Critical Infrastructure Assets

The problem

The current Register framework is too rigid and prescriptive. Part 2 of the SOCI Act sets detailed registration information fields in primary legislation, which makes the framework difficult to update as asset classes, operating models and regulatory needs change.

This limits the ability to tailor Register requirements for different sectors, asset types and reporting entities. Information that is useful for one class of asset may be unnecessary or poorly suited to another, but Act-level prescription means even technical or burden-reducing adjustments may require legislative amendment.

The current change-notification model is also more complex than necessary. It requires entities to assess whether information previously provided has become incorrect or incomplete, rather than requiring notification of clearly prescribed kinds of change. This can make compliance less straightforward, particularly where information was provided some time ago or where ownership, control or operational arrangements have evolved.

> **Proposed model for consultation:** Restructure Part 2 so the Act sets broad categories of registrable information, and the Rules prescribe the specific information items within those categories. The approved form would be the submission mechanism and would not impose information requirements beyond those prescribed in the Rules.
>
> The purpose is to move from highly prescriptive Act-level data fields to a clearer and more adaptable Register framework. This would allow registration requirements to remain proportionate and current over time, while ensuring detailed requirements are set through Rules.

Key design elements

Element	Description
Clear Act and Rules architecture	The Act would establish broad categories of registrable information, while the Rules would prescribe the specific information items within those categories. This would move detailed data fields out of primary legislation and allow requirements to be tailored by asset class, reporting entity or circumstance. The Rules would remain subject to consultation and parliamentary scrutiny, preserving clear limits on the information burden.
Approved form	The approved form would operate as the mechanism for submitting information to the Secretary. It would not be an independent source of legal obligation and would not require information beyond the kinds prescribed in the Rules for the relevant asset class, reporting entity or circumstance.
Simpler notification trigger	The current notifiable-event framework would be replaced with a clearer obligation to notify changes of a kind prescribed in the Rules. The trigger would

Element	Description
	be based on when the entity becomes aware, or ought reasonably to have become aware, of the prescribed change, rather than on a comparison with information previously submitted to the Register. The Rules could prescribe different notification periods for different classes of change.
Tailoring and proportionality	The Rules could prescribe different information requirements and notification settings for different classes of critical infrastructure asset, reporting entity or circumstance. This would allow Register requirements to be calibrated to the relevant asset class and regulatory purpose, rather than applying the same detailed Act-level fields across the framework.
Targeted systems, suppliers and dependencies information	It is intended that the reformed framework would expressly support a category for key systems, key suppliers and material dependencies relevant to the operation, control or continued functioning of the asset. Detailed requirements within that category would be prescribed in the Rules and tailored by asset class or reporting entity, so information is collected only where justified and appropriately limited.
Transition for existing registered entities	Entities that have already provided information under the current Register provisions would not be required to re-register merely because the architecture changes. Information already held on the Register would transition into the new framework. Further information would only be required where prescribed, and subject to appropriate commencement or transition settings.

Preliminary Impact Analysis

This measure is expected to be broadly cost-neutral. It would not change which entities must register, but would make Register obligations clearer and easier to administer for entities already captured under Part 2.

The main costs are expected to be one-off, arising from familiarisation with the revised structure and from updating internal processes so that registrable changes are notified within the required timeframes. Ongoing costs are expected to remain stable or fall, because a clearer structure and Rules-based detail would allow low-value reporting to be removed. The measure is not expected to adversely affect competition, innovation or market entry. The principal driver of ongoing burden is the range of changes treated as notifiable, together with the transition arrangements for entities that have already registered.

Consultation questions

7. Are the proposed broad categories of registrable information clear enough to define the information burden while allowing detailed information items to be prescribed in the Rules?
8. Should the approved form be expressly prevented from requiring information beyond the kinds prescribed in the Rules?
9. What systems, suppliers or dependencies information would be most useful for critical infrastructure visibility, incident modelling and cascading-risk analysis, and what limits should apply?
10. Is a Rules-defined change-notification model more workable than the current notifiable-event framework based on incorrect or incomplete previously submitted information?
11. What notification periods should apply for different classes of change?
12. What transition settings are needed so entities that have already registered do not need to re-register unnecessarily?

Measure 3 – CIRMP Annual Reporting Simplification

The problem

The current CIRMP annual reporting obligation is too rigid because much of the report content is fixed in primary legislation. Section 30AG prescribes detailed matters that must be included in annual reports, while also requiring the report to be given in an approved form. This means reporting content is effectively fixed in two places, and the approved form cannot streamline, remove or reshape information that the Act itself requires.

This limits the ability to keep annual reporting proportionate and useful. Questions that provide limited regulatory value may remain fixed in the Act, and different asset classes, sectors or responsible entities cannot easily be given more tailored reporting requirements without legislative amendment. The current architecture also contributes to complexity because related reporting requirements sit across separate provisions and pathways. This can make the framework harder for responsible entities to navigate, particularly where an entity is subject to different SOCI obligations or operates across multiple asset classes.

Proposed model for consultation: Replace the current section 30AG reporting model with a simpler statutory obligation to give an annual compliance report in an approved form. The Act would continue to impose the reporting obligation, the timing requirement and the governing-body approval requirement. The detailed questions for each reporting period would be set through the approved form rather than hard coded in the Act.

The approved form would operate within clear statutory limits. Reporting questions would need to relate to the entity's compliance with SOCI obligations or to the administration, assurance or enforcement of the Act. Questions would be published in advance so responsible entities can prepare for the relevant reporting period.

The purpose is to make annual reporting more proportionate, predictable and useful by allowing low-value or duplicative questions to be removed, reporting content to be tailored for different entities or assets, and related reporting pathways to be consolidated where appropriate.

Key design elements

Element	Description
Clear statutory obligation with adaptable report content	The Act would impose the obligation to give an annual compliance report, set the timing requirement and retain governing-body approval. Detailed report content would be set through the approved form rather than prescribed in primary legislation. This would allow reporting content to be updated over time without requiring amendment to the Act.
Statutory limits on reporting questions	The approved form would not provide an unconstrained power to require information. Questions would need to relate to the entity's compliance with SOCI obligations or to the administration, assurance or enforcement of the Act. This would preserve clear limits on the reporting burden while allowing reporting content to be adjusted as the framework evolves.
Advance publication of reporting questions	The Department intends to publish reporting questions before the relevant reporting period so responsible entities can prepare.
Tailoring and proportionality	The Rules could allow different reporting requirements for different classes of responsible entity or critical infrastructure asset. This would allow reporting to be calibrated to the relevant obligation, asset class, sector or risk profile, rather than requiring the same detailed report content to apply across all circumstances.
Consolidated reporting pathways	The Department is considering whether annual reporting requirements that currently sit in separate pathways could be consolidated into the redesigned annual reporting framework. The objective would be to reduce complexity by using one reporting architecture, with different questions or requirements applied through the approved form or Rules where needed.
Group reporting	The Department is considering whether a member of a corporate group should be able to lodge a report on behalf of one or more related entities. This could reduce duplicated reporting within corporate groups while still requiring clear information about each responsible entity and critical infrastructure asset.
Governing-body approval	The Act would retain governing-body approval before an annual report is submitted to preserve accountability.

Preliminary Impact Analysis

This measure is expected to be broadly cost-neutral and is deregulatory in intent. It applies to responsible entities that already lodge a CIRMP annual report. It would remove low-value and duplicative questions and allow the report to be updated where compliance and administration require.

The main costs are expected to be one-off, arising from familiarisation with the revised report and from minor updates to internal reporting and board-approval processes. Recurring effort is expected to fall for most entities, because a better-targeted report takes less time to complete and approve. The measure is not expected to adversely affect competition, innovation or market entry, and the saving would accrue across the reporting base in proportion to current effort.

Consultation questions

13. Does the proposed annual reporting model provide a workable way to make reporting more adaptable while preserving clear statutory limits?
14. What matters should remain fixed in the Act, and what matters should be set through the approved form or Rules?
15. How far in advance should proposed reporting questions be published? Would a minimum period of three months before the reporting period provide sufficient predictability?
16. Should corporate groups be able to lodge a consolidated or group-level report where this reduces duplication and still provides clear asset-level and entity-level information?

Measure 4 – Part 2D Notification Clarification

The problem

Part 2D supports Department and industry engagement on changes or proposed changes to critical telecommunications assets that may materially affect the responsible entity's capacity to meet the security obligation in section 30EB. The framework is intended to operate as a continuing notification mechanism for relevant changes, rather than as a project approval process.

In practice, telecommunications projects, systems and service arrangements can evolve after an initial notification is made. Design, procurement, supplier, network, ownership or implementation details may change over time. Where this occurs, it may not always be clear how a written notice from the Secretary under section 30ED applies to later or materially altered aspects of the same project or arrangement.

This can create uncertainty about whether a further notification is required after an earlier section 30ED notice. A section 30ED notice reflects the Secretary's assessment of the notified change, based on the information available at the time. It should not be treated as approval of later stages, future changes or materially different arrangements that were not part of the notified matter and may separately meet the section 30EC threshold.

The reform would preserve the existing notification threshold and assessment framework, while making the legal effect of a section 30ED notice clearer on the face of the Act. This would help responsible entities apply Part 2D more confidently as projects and services evolve, and support more consistent notification of changes that meet the existing statutory test.

Proposed model for consultation: Amend section 30ED to require a written notice from the Secretary to state that the assessment is made at a point in time and on the basis of the information then available.

The notice would also state that it does not remove or limit the responsible entity's obligation to notify again if further changes or proposed changes arise that meet the statutory threshold in section 30EC.

The purpose of the amendment is to give responsible entities greater certainty about the legal effect of a section 30ED notice. The existing statutory test for notification would be preserved. The assessment would remain confined to the matter notified and would not operate as approval of a broader project, future stage, later change or materially altered arrangement.

Key design elements

Element	Description
Point-in-time assessment	Section 30ED notices would be required to state that the Secretary's assessment is made at a point in time and on the basis of the information then available. This would make clear that the notice relates to the notified change or proposed change, not to future stages or later variations of a project or arrangement.
Continuing notification obligation	The notice would state that it does not remove or limit the responsible entity's obligation to notify further changes or proposed changes that separately meet the threshold in section 30EC. This would help responsible entities assess when a later project, system, service, ownership or implementation change may require a further notification.
Applies to both forms of notice	The clarification would apply whether the Secretary's notice identifies a risk or indicates that no risk is identified. In either case, the notice would not operate as approval for later changes or materially altered arrangements that were not assessed on the information before the Secretary.
Civil penalty setting	The Department is considering whether the civil penalty for breach of section 30EC should be increased to better reflect the importance of timely notification of material changes affecting critical telecommunications assets. The proposed clarification would support more consistent application of the existing obligation by making the effect of section 30ED notices clearer.
What is not changing	The reform would not expand the scope of section 30EC or change the substantive threshold for notification. The responsible entity would continue to assess whether a change or proposed change is likely to have a material adverse effect on the asset's capacity to comply with the security obligation in section 30EB.

Preliminary Impact Analysis

This measure would clarify the effect of a section 30ED notice for responsible entities for critical telecommunications assets, including when a later or materially different change may require a further notification. It would capture no new entities and would operate within the existing Part 2D framework.

The main costs are expected to be one-off, comprising familiarisation and an update to internal change-assessment processes. A clearer statement of the notice's legal effect is expected to reduce unnecessary repeat or precautionary notifications, lowering ongoing effort for entities that make frequent network or supplier changes while still capturing later changes that meet the statutory threshold. The measure is not expected to adversely affect competition, innovation or market entry. The value of the measure would depend on whether the clarified notice effect gives entities sufficient certainty to plan network and supplier changes.

Consultation questions

17. Does the proposed clarification make the legal effect of a section 30ED notice sufficiently clear?
18. What practical issues arise in determining when a later project, design, system, service, supplier or ownership change is sufficiently different or material to require a further notification under section 30EC?
19. What guidance or examples would help responsible entities apply the continuing notification obligation where a project or arrangement evolves after an earlier section 30ED notice?
20. Are there particular categories of change for which further guidance would be useful, such as changes to suppliers, network architecture, managed services, offshore arrangements, ownership or operational control?
21. Is an increase in the civil penalty for non-compliance with section 30EC appropriate to reflect the importance of timely notification? If not, what alternative approach should be considered?

Measure 5 – Cyber Security Incident Definition: Automated Systems, Software Agents and AI

The problem

The SOCI Act uses the term "cyber security incident" to determine when certain reporting, preparedness and response obligations apply. The term is defined in section 12M by reference to unauthorised access, modification or impairment involving computer data, computer programs, electronic communications or computers. Section 12N explains when that access, modification or impairment is unauthorised.

The definition is most visible in Part 2B, which requires responsible entities to notify certain cyber security incidents affecting critical infrastructure assets. It is also used in other parts of the Act, including enhanced cyber security obligations for systems of national significance and the serious incident response framework. The main practical issue for this measure is to ensure that responsible entities can identify and report cyber security incidents involving emerging technologies where those incidents cause relevant harm.

The current definition works for many conventional cyber incidents, including intrusion, malware, unauthorised access and other forms of cyber interference. However, critical infrastructure systems are becoming more automated and software-dependent. Serious cyber incidents may increasingly involve automated systems, software agents, AI-enabled tools or comparable technologies.

Automation does not necessarily change the cyber security character of an incident. A serious cyber incident should not fall outside the definition merely because the relevant access, modification or impairment is caused by or through an automated system, rather than directly by an identifiable natural person. The current definition may create uncertainty in those cases, particularly where attribution is difficult or the automated mechanism obscures who caused the relevant access, modification or impairment.

A related issue arises where an automated or AI-enabled system is authorised for use in connection with a critical infrastructure asset, but is compromised, manipulated or materially uncontrolled in a way that causes cyber-related harm to the asset or to systems used in connection with it. In those circumstances, it may be unclear whether the incident involves unauthorised conduct, even where the practical effect is comparable to an incident the SOCI framework would otherwise be expected to address.

The policy problem is one of clarity and future-proofing. Serious cyber security incidents should remain within the SOCI framework where automation, software agents, AI-enabled tools or comparable technologies affect how the incident occurs, how it is attributed, or how it causes harm. At the same time, the definition should not create a general AI incident regime or capture ordinary software defects, configuration issues, routine outages, model errors or general technology failures merely because automation or AI is involved.

Proposed model for consultation: Amend the definition of "cyber security incident" in section 12M, and any supporting concepts in section 12N if required, so that the definition operates clearly where serious cyber security incidents involve automated systems, software agents, AI-enabled tools or comparable technologies.

The amendment would clarify that unauthorised access, modification or impairment is not excluded merely because it is caused by or through an automated system, software agent, AI-enabled tool or comparable technology. The focus would remain on whether the access, modification or impairment is unauthorised in substance, and whether the relevant statutory consequences or thresholds are otherwise met.

The amendment would also address serious incidents involving authorised automated or AI-enabled systems where the system is compromised, manipulated or materially uncontrolled in a way that causes cyber-related harm to the asset or to systems used in connection with it. The purpose is to deal with cases where the system is authorised to operate, but the harmful conduct or effect is not authorised in substance.

Because "cyber security incident" is a defined term used in more than one part of the SOCI Act, the amendment would need to work wherever that term is used. The main practical effect would be on Part 2B incident notification. The amendment would also need to preserve the intended operation of related provisions, including enhanced cyber security obligations for systems of national significance and the serious incident response framework. It would not change the separate thresholds or safeguards that apply in those parts of the Act.

The amendment would not change the existing Part 2B impact thresholds in sections 30BC and 30BD. Responsible entities would still only be required to report cyber security incidents that meet the relevant statutory reporting thresholds. The amendment would clarify whether an event is capable of being a cyber security incident before those reporting thresholds are applied.

The amendment is not intended to create a separate reporting regime for AI incidents, automated decision-making incidents or general technology failures. Ordinary software bugs, routine outages, model errors, configuration mistakes or technology failures would not be captured merely because an automated or AI-enabled system is involved. The incident would still need to have a cyber security character.

Key design elements

Element	Description
Definition-level amendment	The reform would amend the definition of "cyber security incident" in section 12M, and supporting concepts in section 12N if required. The amendment would

Element	Description
	be made at the definition level so the concept remains clear and consistent across the SOCI Act.
Main practical effect: incident triage and reporting	The main practical effect would be to help responsible entities classify incidents consistently for Part 2B reporting. Responsible entities would be better able to assess whether an incident involving automation, software agents, AI-enabled tools or comparable technologies is a cyber security incident and, if so, whether it meets the existing reporting thresholds. Because the term is also used elsewhere in the Act, consequential review would ensure related provisions continue to operate as intended. This includes enhanced cyber security obligations for systems of national significance and the serious incident response framework. The amendment would not change the separate thresholds, safeguards or decision-making requirements that apply under those provisions.
Unauthorised conduct caused by or through automated systems	The Act would clarify that access, modification or impairment is not excluded from the definition merely because it is caused by or through an automated system, software agent, AI-enabled tool or comparable technology. The existing role of authority and entitlement would be preserved.
Compromised or materially uncontrolled authorised systems	The definition would address serious incidents involving authorised automated or AI-enabled systems where the system is compromised, manipulated or materially uncontrolled in a way that causes cyber-related harm. This would address cases where the system is authorised to operate, but the harmful conduct or effect is not authorised in substance.
Cyber security character	The amendment would preserve the cyber security character of the definition. It would not convert ordinary software defects, configuration issues, routine outages, model errors, technology failures or non-security AI issues into cyber security incidents merely because automation or AI is involved.
Part 2B thresholds preserved	The reform would not change the existing Part 2B reporting thresholds in sections 30BC and 30BD. The clarification would affect whether an event is capable of being a cyber security incident. It would not alter the additional requirements that determine whether a responsible entity must report a critical cyber security incident or other cyber security incident.
No separate AI incident regime	The reform would not create a separate AI incident reporting regime or a general technology incident regime. It would refine the existing cyber security incident definition so that it continues to operate effectively where automation changes how a cyber incident occurs or makes attribution less straightforward.
Consequential amendments and guidance	Consequential amendments may be needed to ensure that references to cyber security incidents across the Act operate as intended. Guidance and examples would support responsible entities in distinguishing cyber security incidents involving automation from ordinary technology failures, software defects, configuration issues or non-security AI issues.

Preliminary Impact Analysis

This measure would clarify the definition of "cyber security incident" so that responsible entities can classify incidents consistently where automated systems, software agents, AI-enabled tools or comparable technologies are involved. The main practical impact would be on entities already subject to Part 2B incident notification obligations.

The measure would adjust the scope of an existing statutory concept rather than create a new standalone obligation. For Part 2B, responsible entities would still only be required to report incidents that meet the existing statutory impact thresholds. For other parts of the Act that use the term "cyber security incident", consequential review would ensure the revised definition operates as intended without changing separate statutory thresholds or safeguards.

The main costs are expected to be one-off. They would include familiarisation with the revised definition, updates to incident triage and escalation processes, and guidance or training so that affected incidents are classified consistently. Entities with mature security operations are expected to absorb this within existing incident-response arrangements.

The clarification may reduce the risk of inconsistent or omitted reporting where automation affects the mechanism, attribution or operation of a cyber incident. The measure is not expected to adversely affect competition, innovation or market entry, provided the definition remains confined to incidents with a cyber security character and does not capture ordinary software defects, routine outages or general technology failures.

Consultation questions

22. Does the proposed definition-level clarification make clear when a cyber security incident involving automated systems, software agents, AI-enabled tools or comparable technologies should be treated as a cyber security incident under the SOCI Act?
23. Does the proposed approach preserve the cyber security character of the definition, including by excluding ordinary software defects, configuration issues, routine outages, model errors, general technology failures and non-security AI issues?
24. How should the legislation deal with incidents involving authorised automated or AI-enabled systems that are compromised, manipulated or materially uncontrolled in a way that causes cyber-related harm?
25. What guidance, examples or consequential amendments would help responsible entities apply the revised definition consistently, including for Part 2B reporting?

A.3 – Simplifying enhanced-obligation architecture

Measure 6 – Systems of National Significance

The problem

The current Systems of National Significance (SoNS) framework can be difficult for responsible entities to navigate. When an asset is declared to be a SoNS, it may not be clear at that point what additional obligations will apply, when they will commence, or how the entity's existing preparedness arrangements will be treated. This is because declaration and the application of enhanced obligations operate through separate processes.

This can create uncertainty for industry about what designation will require, when obligations will commence, and how existing continuity, crisis management, recovery, exercise or equivalent regulatory arrangements will be taken into account. It can also lead to duplicated engagement and additional administrative effort before entities have a complete picture of the obligations that would apply. For entities that already maintain mature preparedness arrangements, the current framework does not provide a sufficiently clear pathway for recognising those arrangements while identifying and addressing any material gaps.

The current SoNS incident response planning obligation is also narrower than the preparedness outcomes expected for nationally significant assets. It focuses on cyber incident response, rather than the broader ability of the declared asset to maintain critical functions, manage disruption, recover, restore operations and resume services. Those outcomes are particularly important for assets whose disruption could have significant national consequences.

The vulnerability assessment framework is also framed too narrowly and can be difficult to apply in a timely and targeted way. It is currently tied to cyber security incident concepts, which may not support assessment of other material vulnerabilities affecting a declared asset, including physical, personnel, supply chain, natural hazard or other operational risks.

Together, these issues can make SoNS designation harder to understand, more administratively burdensome, and less clearly focused on the practical preparedness of nationally significant assets.

Proposed model for consultation: Simplify the SoNS framework so responsible entities have a clearer understanding of what designation means in practice. The model would include an asset-specific resilience planning obligation and cyber security exercises, with commencement, implementation and transition settings calibrated to the asset, risk profile and existing arrangements.

The current incident response planning obligation would be replaced with a resilience planning obligation focused on continuity, recovery, restoration and resumption of the declared asset's critical functions or services. Vulnerability assessments would be retained as a discretionary all-hazards tool, rather than an automatic consequence of designation. The System Information ECSO would be repealed.

The framework would include a clearer mechanism to recognise existing plans, exercises, continuity arrangements or equivalent regulatory requirements that already apply to the declared asset, while preserving the ability to identify and address any material gaps.

The intention is to create a simpler and more predictable SoNS architecture that gives responsible entities clearer expectations, supports preparedness for nationally significant assets, and reduces unnecessary duplication.

Key design elements

Element	Description
Baseline consequence of declaration	The declaration process would give responsible entities a clearer picture of what follows from SoNS designation. It would identify the obligations that apply, or are expected to apply, and the relevant commencement, compliance and transition settings. This would help responsible entities plan for implementation from the point of designation.
Calibrated implementation and transition	Not every obligation would need to be enforceable immediately upon declaration. Implementation periods could be calibrated having regard to the nature of the obligation, the responsible entity's existing arrangements, the urgency of the risk, and whether equivalent arrangements already apply. This would support timely uplift while giving entities a workable pathway to compliance.
Streamlined consultation process	Consultation on designation and on proposed SoNS obligations could occur concurrently. A single consultation process, or coordinated notices issued together, could identify the proposed declaration, the obligations that would apply, relevant implementation settings, and any pathway for recognising equivalent arrangements. This would reduce duplicated engagement and give responsible entities a clearer view of the whole proposal.
Asset-specific resilience planning	The resilience planning obligation would replace the current SoNS incident response planning obligation. It would require the responsible entity to maintain arrangements for managing disruption affecting the declared asset, maintaining or restoring its critical functions, and supporting recovery, restoration and resumption of services.

Element	Description
	The obligation would be directed to the declared SoNS asset and its critical functions or services. It would not impose an enterprise-wide crisis management obligation unrelated to the declared asset. A responsible entity could rely on existing continuity, crisis management, recovery, operational resilience or equivalent documents to the extent they adequately address the declared asset.
Cyber security exercises	Cyber security exercises would operate as an enduring consequence of designation, with implementation settings calibrated to the declared asset and existing arrangements. Exercises would support testing and improvement of the asset's preparedness arrangements and could be aligned with existing exercise programs where they deliver substantially equivalent outcomes.
Discretionary and targeted all-hazards vulnerability assessments	Vulnerability assessments would remain discretionary and would not arise automatically upon designation. They would be reframed on an all-hazards basis so they can address material vulnerabilities affecting the declared asset, including cyber and information security, physical security, personnel security, supply chain security, natural hazards or other relevant sources of risk. The power would be used in a targeted way, including by reference to specific vulnerabilities, classes of vulnerability, asset-specific or sector-specific threat information, or threat advice from an intelligence agency or other relevant Commonwealth body.
Proportionate follow-up action	Where a vulnerability assessment identifies a material vulnerability or deficiency affecting the declared asset, the framework would support proportionate follow-up action. This could include requiring a remediation plan, specified remedial measures, updates to the resilience plan or equivalent documents, or a report on action taken. Follow-up action would be directed to identified material gaps rather than general uplift unrelated to the assessment.
Recognition of equivalent frameworks	The framework would allow existing plans, exercises, continuity arrangements or equivalent regulatory requirements to be recognised where they impose substantially equivalent or stronger requirements for the declared asset. A responsible entity could identify the relevant plan, instrument or arrangement, and the Secretary could require material to be provided where needed to assess equivalence. Where a material gap is identified, the responsible entity could be required to supplement, vary or adapt the existing arrangement rather than prepare a wholly separate SoNS-specific document.
Repeal of the System Information ECSO	The System Information ECSO would be repealed. This would remove a feature of the current framework that has proven difficult to operate.
Continuity where responsibility for an asset changes	Because SoNS obligations attach to the declared asset, continuity arrangements would be needed where responsibility for the asset changes through sale, transfer, outsourcing, restructure or another change in control or operation. The outgoing responsible entity would notify the Secretary, and the incoming

Element	Description
	responsible entity would have a prescribed period to adopt, maintain or identify the resilience plan or equivalent documents applying to the asset.
Transition for existing SoNS assets	Existing SoNS declarations should continue in force after commencement. Existing incident response planning obligations should continue in force and transition into the new resilience planning framework. Existing exercise and vulnerability assessment notices should also continue in force. Assets already declared as SoNS should be given an appropriate implementation period to prepare, adopt or identify a resilience plan or equivalent document.
What is not changing	The reform would not alter the threshold for declaring an asset to be a SoNS. It would simplify the process, make the practical consequences of designation clearer, and create a more coherent and less duplicative preparedness framework. The resilience planning obligation would remain focused on the declared asset and its critical functions or services, rather than imposing a general enterprise-wide obligation.

Preliminary Impact Analysis

This measure would apply only to assets declared to be SoNS under the existing declaration threshold, a small and individually selected group. For those entities it would make the consequences of designation clearer and more predictable. It may reduce regulatory cost where existing continuity, crisis-management, recovery or exercise arrangements can be recognised, and where repeal of the System Information ECSO removes an unused compliance pathway.

Regulatory costs may increase for some declared entities. This may occur where existing cyber incident response plans need to be expanded into asset-specific resilience planning, where cyber security exercises require additional preparation, and where targeted vulnerability assessments identify material gaps that require remediation. One-off costs would include familiarisation, updating plans and governance processes, and addressing identified deficiencies. Some enhanced obligations, such as participation in cyber security exercises and periodic vulnerability assessments, would recur. Because the population is small and individually assessed, these costs are concentrated and can be calibrated to each entity.

The measure is not expected to directly affect competition, innovation or market entry, because it applies only to assets declared to be Systems of National Significance. The scale of cost would depend on how readily equivalent existing arrangements are recognised and on the transition arrangements provided to meet the enhanced obligations.

Consultation questions

26. What implementation period should apply before new SoNS resilience planning or cyber security exercise obligations become enforceable for newly declared SoNS assets?
27. How should the framework recognise existing continuity, crisis management, recovery, exercise or equivalent regulatory arrangements that already apply to a declared SoNS asset?
28. What information should a responsible entity provide when relying on an existing plan, document or regulatory framework as substantially equivalent?
29. How should material gaps in existing arrangements be identified and addressed without requiring unnecessary duplication?
30. Is the proposed resilience planning obligation appropriately focused on the declared asset and its critical functions or services?
31. What guidance or examples would help responsible entities understand the practical consequences of SoNS designation?
32. Should vulnerability assessments remain discretionary and be reframed on an all-hazards basis? What limits or safeguards would ensure they remain targeted and proportionate?
33. What transitional settings are needed for existing SoNS assets as current incident response planning obligations transition into the proposed resilience planning framework?

A.4 – Clarifying uncertain asset boundaries

Measure 7 – Submarine Telecommunications Cables and Associated Infrastructure

The problem

Australia relies on submarine cable systems to support telecommunications, data services, government operations, financial markets and many other critical infrastructure sectors. Disruption, degradation or compromise of a nationally significant cable system can affect the continuity and resilience of multiple dependent services.

The current SOCI framework does not always align clearly with the way modern submarine cable systems are structured and operated. It assumes a more traditional model in which relevant infrastructure is owned or operated by a carrier or carriage service provider. In practice, cable systems may be held through consortia, special purpose vehicles, neutral host arrangements or other multi-party structures.

This can make the framework difficult to apply where important physical or operational functions sit with entities that are not carriers or carriage service providers. Those functions may include landing infrastructure, cable landing stations, terminal equipment, power feed equipment, network management systems or other supporting operational systems. Where that occurs, the current framework may not clearly identify the relevant asset or the entity responsible for managing the associated security or resilience risk.

The current framework also leaves uncertainty about the physical and operational boundary of a cable system. The current Schedule 3A concept focuses mainly on the cable on or beneath the seabed. It does not clearly identify which shore-end, landing, terminal, power, network-management or supporting operational components should be treated as part of the cable system for SOCI purposes, including where facilities are shared or operational components are physically separated.

A further issue is that the current direct interest holder framework does not adequately reflect the way interests are held in modern cable systems. Long-term capacity arrangements, including indefeasible rights of use and similar arrangements, may confer substantive influence, exclusivity or dependency without fitting neatly within existing ownership concepts. At the same time, ordinary wholesale, enterprise or customer capacity arrangements should not be treated as direct interests merely because they involve use of cable capacity.

Together, these issues can make it unclear what parts of a nationally significant submarine cable system are regulated, which entity is responsible for each part, and how significant commercial interests in the system should be treated. They can also create uncertainty for ordinary capacity users and operators of unrelated infrastructure located in the same facility.

Proposed model for consultation: Refine the existing critical telecommunications asset framework so it can apply more clearly to nationally significant submarine cable systems with an Australian landing, including associated physical and operational components that are essential to the operation, security, resilience or restoration of the system.

The reform would work within the existing critical telecommunications asset framework. It would not create a standalone submarine cable sector. Critical cable infrastructure would be identified by function, and obligations would attach to the owner or operator of the relevant component or function rather than turning primarily on whether that entity is a carrier or carriage service provider.

Under the model being considered, the asset boundary could include the submarine cable itself and associated shore-end, landing, terminal, power feed and network-management components where those components form part of the operational cable system. Co-located infrastructure or services would not be captured merely because they are in the same facility.

A single cable system may involve more than one responsible entity where ownership or operational responsibility is distributed. Each responsible entity would be responsible for the component or function it owns or operates.

The reform would also update the treatment of relevant interests in cable systems. Long-term capacity arrangements, indefeasible rights of use, consortium rights and similar arrangements could be treated as relevant interests where they give a person substantive influence, exclusivity or dependency relevant to the operation, security or resilience of the cable system. Ordinary wholesale, enterprise or customer capacity arrangements would not be treated in this way merely because they involve use of cable capacity.

The policy intent is to align SOCI obligations with the parts of a nationally significant cable system that matter to its operation, security, resilience and restoration. The reform is not intended to create a general regime for ordinary capacity users.

Key design elements

Element	Description
System-based treatment within the telecommunications framework	The reform would operate within the existing critical telecommunications asset class, while allowing a nationally significant submarine cable system with an Australian landing to be treated more coherently as a critical telecommunications system for SOCI purposes. The intention is not to create a new standalone submarine cable sector; it is to make the existing telecommunications framework clearer for cable systems that are owned, operated or controlled through contemporary commercial structures.
Functional asset boundary	Capture could extend beyond the seabed cable itself to associated physical and operational components that are essential to the operation, security, resilience or restoration of the cable system. This could include repeaters, branching units and other devices attached to the cable, the cable landing point, beach manholes, shore-end conduit, cable landing station components, submarine line terminal equipment, power feed equipment, and network-management, branch-management control or line-monitoring systems, where those components are used in the operation of the cable system.
Limits for shared and co-located facilities	The boundary would not capture unrelated infrastructure or services merely because they are in the same facility as cable-related equipment. For shared cable landing stations or neutral host facilities, the framework would focus on the components, systems or functions that are genuinely used in the operation of the relevant cable system.
Responsible entity for relevant components or functions	The responsible entity would be the owner or operator of the relevant component or function, regardless of whether that entity is a carrier or carriage service provider. A single cable system may involve more than one responsible entity where ownership or operational responsibility is distributed. Each responsible entity would be responsible for the component or function it owns or operates and would not be responsible for infrastructure it does not own or operate.
Coordination across distributed responsibility	Where different entities own or operate different components of the same cable system, each entity would be responsible for its own component or function. Coordination risks and interdependencies could be addressed through relevant risk management obligations, including requirements for each responsible entity's CIRMP to address risks arising from interdependence with other components of the same cable system and with other responsible entities.
Cable landing station boundary	The boundary for cable landing stations would be drawn by function, not by physical partition. A cable landing station could be captured to the extent that it houses equipment used in the operation of the relevant cable, including relevant power, cooling, physical security systems and dedicated cable entry infrastructure. Co-located infrastructure or services would not be captured merely because they are in the same facility.

Element	Description
Contemporary ownership and operating arrangements	The reform would work with modern industry structures, including consortia, special purpose vehicles, neutral host arrangements and outsourced operations. The scope of capture would turn on what the component does, and who owns or operates it, rather than on corporate structure or carrier or carriage service provider status alone.
Targeted treatment of material cable interests	The treatment of direct interest holders would be updated so that long-term capacity arrangements, indefeasible rights of use, capacity leases, consortium rights or similar arrangements can be addressed where they confer substantive influence, exclusivity or dependency relevant to the operation, security or resilience of the cable system. Ordinary wholesale, enterprise or customer capacity arrangements would not be treated as direct interests merely because they involve use of cable capacity.
What is not changing	The reform would not displace the existing telecommunications framework or create a separate new regime for submarine cable systems. It would not treat ordinary wholesale, enterprise or customer capacity users as direct interest holders merely because they use cable capacity. It would not capture unrelated infrastructure or services merely because they are co-located with cable-related equipment.

Preliminary Impact Analysis

This measure is likely to result in additional entities becoming subject to SOCI obligations where they own or operate the components of a nationally significant submarine cable system that are most relevant to its security and restoration, including shore-ends, landing stations, terminal equipment, power feeds and network management. Australia is connected by approximately 18 in-service international cable systems, which land at a small number of concentrated sites, principally in northern and southern Sydney and Perth, with further landings at the Sunshine Coast and Darwin. Ownership is held by a limited set of carriers and consortia. The measure may also affect holders of long-term capacity, indefeasible rights of use or consortium rights where those interests confer substantive influence or dependency, but will not affect ordinary users who purchase cable capacity.

The expected costs comprise both one-off transition costs and ongoing compliance costs. One-off costs arise from assessing the cable system boundary, identifying the responsible entity for each relevant component, registering newly captured assets or interests, and establishing the risk management arrangements and controls needed to meet SOCI obligations. Because the measure may bring entities into the regime for the first time, those entities would also incur ongoing costs in maintaining and updating their risk management programs, undertaking annual reporting, and meeting cyber incident reporting and register obligations. Some entities may also incur coordination costs, both initial and ongoing, where responsibility for a single cable system is distributed across several owners, which is common under the consortium ownership model for international cables.

The measure is expected to have a limited effect on competition, innovation or market entry, because it is directed to nationally significant cable systems and to entities with ownership or operational control over their critical components. The number of in-scope landing stations and shore facilities is small and

identifiable. The principal variables for impact are the treatment of shared facilities and long-term capacity arrangements, and the transition period available to newly captured entities.

Consultation questions

34. Is the proposed function-based cable system boundary workable, including for submarine cable, shore-end, landing, terminal, power feed and network-management components used in the operation of a nationally significant submarine cable system? What limits or exclusions are needed?

35. How should the boundary of a cable landing station or shared facility be drawn, including where cable-related components are co-located with unrelated infrastructure or physically separated from other operational components?

36. Are the proposed responsible-entity principles workable where ownership, operation or control of different components is distributed across consortia, special purpose vehicles, neutral host arrangements or outsourced operators? How should interdependencies between responsible entities be addressed?

37. What features should distinguish long-term capacity arrangements, indefeasible rights of use, capacity leases, consortium rights or similar arrangements that create SOCI-relevant influence, exclusivity or dependency from ordinary wholesale, enterprise or customer capacity arrangements?

38. What transition period, guidance or worked examples would newly captured owners, operators or material interest holders need to understand and comply with any new registration, notification or risk management obligations?

Measure 8 – Data Storage or Processing Capture Pathways

The problem

The current definition of “critical data storage or processing asset” no longer provides a clear, self-assessable basis for identifying nationally significant data storage or processing facilities and services. It does not align well with contemporary operating models for multi-tenant data centres, hyperscale and colocation facilities, cloud services, managed hosting and other service layers.

The current definition identifies assets indirectly, by reference to customer identity, the handling of business-critical data and the provider’s knowledge of how the service is used. Those matters may be relevant to risk assessment, but they are not well suited to operating as the primary capture test for contemporary data infrastructure. In practice, they depend on information that may sit with the customer rather than the provider, including the customer’s regulatory status, the downstream use of the service, the sensitivity or criticality of particular datasets, and whether the customer has notified the provider.

This creates uncertainty for providers and can produce inconsistent outcomes. Significant facilities or service-layer providers may be outside the framework if the customer-driven criteria are not met or if notification does not occur. Conversely, a service may be captured because of an individual customer relationship or data characterisation, rather than because of the scale, role or systemic significance of the facility or service itself.

The result is that providers may not be able to determine their SOCI status from their own facilities, services or certifications. This makes the framework less predictable, increases reliance on customer notification

under subsection 12F(3), and can misalign regulation with the facilities and services that are significant in their own right.

These issues point to a need for a clearer way to identify significant data storage or processing facilities and services, without treating all data centres, cloud services or data services as critical infrastructure.

Proposed model for consultation: Replace the current customer-driven capture model in section 12F with a multi-pathway framework that identifies critical data storage or processing assets through clearer provider-facing criteria that entities can assess by reference to their own facilities, services or certifications.

The first three pathways would be objective and provider-facing, so entities can assess their status by reference to their own facilities, services or certifications. They would address significant data-centre facilities, larger service-layer providers and certain certified hosting providers. A fourth, limited Ministerial designation pathway would operate as a reserve mechanism for exceptional cases of government dependency that fall outside the ordinary thresholds.

Regulatory capture would no longer depend primarily on awareness of customer relationships or notification under subsection 12F(3). Customer identity and the character of data handled would not be disregarded, but they would no longer operate as the primary ordinary perimeter for facility-based or service-based capture.

The pathways would be alternative entry points into one regulatory regime. If an entity is captured under more than one pathway, the obligations would apply once rather than cumulatively.

The policy intent is to modernise the existing critical data storage or processing asset class. It is not to create a separate new sector or make all data centres, cloud services or data services critical infrastructure.

Broader Government work on data centres and AI infrastructure: The proposed SOCI reforms would operate alongside broader Government work on data centres and AI infrastructure. The Government's *Expectations of data centres and AI infrastructure developers* are intended to guide project proponents on matters such as national interest, security and resilience, and sustainable development. Those expectations do not create SOCI obligations and do not determine whether an asset is a critical data storage or processing asset. The proposed SOCI reforms are directed to the security and resilience of facilities and services whose scale, role or certification status means that disruption, compromise or prolonged unavailability could have significant consequences for Government, the economy or national security.

Proposed pathways

Pathway	How it works	What it is intended to capture	Starting point for consultation
Facility-based capture	Capture would be based on the physical and operational characteristics of a data-centre facility, measured principally by	Major shared physical infrastructure whose scale and concentration make it systemically significant,	A proposed starting point of 1 MW rated IT load, subject to consultation and refinement using Australian market data. This starting point is informed by

Pathway	How it works	What it is intended to capture	Starting point for consultation
	rated IT load. The pathway would be directed to shared, colocation or otherwise externally provided facilities, rather than internal enterprise systems used solely for the owner's own purposes.	regardless of customer identity.	international comparator work, including the United Kingdom's proposed approach to third-party data centres. The Department recognises that Australian market structure may differ from the United Kingdom and is seeking evidence on whether 1 MW appropriately identifies systemically significant facilities in Australia, whether different thresholds should apply to different facility types, and how rated IT load should be defined and measured.
Service-based capture	Capture would be based on the type and scale of service provided, rather than on whether the provider operates the underlying physical infrastructure. This pathway would be directed to service-layer providers that provide data storage or processing services on a commercial basis and meet a prescribed Australian-facing scale threshold.	Larger cloud, hosted infrastructure, managed hosting, backup and disaster recovery, and comparable service-layer providers whose scale and role make them systemically significant. It is not intended to capture services where data handling is merely incidental.	Thresholds would be set by the Rules, potentially by reference to Australian revenue from in-scope services, customer numbers, data volume, employee headcount or a combination of these.
Certification-based capture	Capture would be based on objective certification held by the provider for a relevant facility or service, rather than on customer identity or service knowledge. The principal model under consideration is certification under the Commonwealth Hosting Certification Framework or an equivalent prescribed scheme.	Providers whose relevant facilities or services are already recognised as suitable for handling sensitive Government information, and whose significance can therefore be established through that certification status.	Current certification under the Hosting Certification Framework, with scope for prescribed equivalent schemes and consultation on whether capture should apply only to certified facilities or services.

Pathway	How it works	What it is intended to capture	Starting point for consultation
Reserve Ministerial designation	A limited reserve mechanism would allow the Minister for Home Affairs to designate a provider supplying services to government where the provider is not captured under the ordinary thresholds and disruption, compromise or prolonged unavailability could have significant consequences for the security or functioning of government. The reserve mechanism would be distinct from the secrecy-based section 51 declaration model.	Exceptional cases of Government dependency that are not adequately captured by the objective facility, service or certification pathways.	A narrow reserve pathway, with consultation on statutory criteria, affected-entity consultation, referral mechanisms, reasons where appropriate, review or revocation arrangements, and transition periods.

Key design elements

Element	Description
Existing asset class, modernised capture model	The reform would modernise how the existing class of critical data storage or processing assets is identified. It would not create a separate new sector or a second parallel data regime. The revised model would identify facilities and services whose scale, role, certification status or exceptional Government dependency warrants SOCI regulation.
Data centre concept	The Act would introduce a broader concept of a data centre as a physical facility, or group of structures, that houses, connects and operates relevant IT equipment together with supporting infrastructure such as power, cooling, security and resilience systems. The concept would accommodate campus-style and distributed designs where multiple structures operate as one integrated facility. It is not intended to capture ordinary office server rooms or incidental internal IT spaces.
Rated IT load	The facility-based pathway would require a clear method for defining and measuring rated IT load. The Department is seeking views on whether this should be based on design capacity, installed capacity, contracted capacity, operational capacity or another measure that can be applied consistently.
Aggregation for campus-style facilities	Multiple buildings, halls, compounds or structures could be treated as one facility where they operate as a single integrated operational unit. Relevant considerations would include common operation, shared essential infrastructure,

Element	Description
	operational interdependence and integrated security and resilience systems. Physical proximity or common ownership alone would not be enough.
Operator-facing pathways	Most providers would be able to assess their status by reference to their own facilities, services or certifications. They would not need to rely primarily on customer identity, customer regulatory status, data characterisation or customer notification. This is the core difference from the current section 12F model.
Australian nexus for service-layer providers	The service-based pathway would apply to larger service-layer providers that provide data storage or processing services on a commercial basis and meet a prescribed Australian-facing scale threshold. This could include cloud, hosted infrastructure, managed hosting, backup and disaster recovery, and comparable service-layer providers. For foreign-domiciled or foreign-headquartered providers, the threshold would operate by reference to Australian-derived revenue or another Australian-facing metric, rather than global group scale. This would better align capture with the provider's significance in the Australian market.
Certification-based capture	Certification-based capture would apply by reference to certification held for a relevant facility or service, such as certification under the Commonwealth Hosting Certification Framework or an equivalent prescribed scheme. The Department is seeking views on whether capture should apply only to the certified facility or service, or to the provider more broadly.
Reserve Ministerial designation	The designation pathway would be narrow and residual. It would be available for exceptional government-dependent cases that fall outside the ordinary facility, service and certification pathways, where disruption, compromise or prolonged unavailability could have significant consequences for the security or functioning of Government. Safeguards could include statutory criteria, affected-provider consultation, referral mechanisms, reasons where appropriate, review or revocation arrangements, and transition periods.
Repeal of customer notification	Because the revised model would use operator-facing capture pathways, the reform would repeal the subsection 12F(3) obligation for critical infrastructure assets to notify commercial data storage or processing providers that they are storing or processing business-critical data. Capture would instead depend on the provider's own facility characteristics, service scale, certification status or designation.
Interaction with section 9(7)	The current requirements of subsection 9(7) would be preserved. That provision deals with data storage or processing systems that form part of another primary critical infrastructure asset. Preserving it would allow internal systems supporting another primary asset to continue to be dealt with under that asset's framework, while the reformed section 12F model applies to external facilities and service providers.

Element	Description
Single set of obligations	If an entity is captured through more than one pathway, the obligations would apply once, not cumulatively. The pathways are different ways into the same regime, not separate overlapping compliance layers.
Exclusions and lower-consequence services	Detailed exclusions would be developed through Rules consultation. The starting point is that ordinary software licensing, professional services, advisory services, incidental data handling and lower-consequence services should not be captured unless they meet a prescribed pathway.
Transition for currently captured and newly captured entities	Entities currently captured under section 12F would transition without an intended gap in coverage if they continue to meet the revised criteria. Some entities currently captured only because of customer notification may fall outside scope. Some facilities or service providers that are not currently captured may come into scope for the first time because of their facility characteristics, service scale, certification status or designation. Newly captured entities would be given a reasonable transition period.
What is not changing	The reform would not make all data services critical infrastructure. Lower-consequence services, incidental data handling and ordinary software or professional services would remain outside scope unless they meet a prescribed pathway.

Interaction with Hosting Certification Framework reforms: The Government is also considering reforms to the Hosting Certification Framework (HCF). Any changes to the HCF may affect the proposed certification-based pathway, including which certifications or equivalent schemes should be recognised for SOCI purposes.

Preliminary Impact Analysis

This measure would change which data storage and processing assets are regulated under SOCI. The size of the affected population depends substantially on where the facility threshold is set. A threshold in the order of 1 MW of rated IT load is low relative to industry norms, because commercial colocation and hyperscale facilities typically operate from approximately 15 MW to well over 100 MW. Such a threshold is likely to capture most commercial facilities while excluding small edge sites and on-premises server rooms. Australia's commercial data-centre base is concentrated in Sydney and Melbourne and operated by a relatively small number of providers. Some entities currently captured only because of customer identity or data characterisation would fall outside scope once the customer-notification model is repealed, which is a deregulatory benefit.

The final population would depend on Rules-level settings, including the facility threshold, service-based metrics, certification settings and the treatment of low-consequence or incidental services. The interaction with the Hosting Certification Framework is significant, because operators that hold a strategic hosting certificate already work to a known assurance baseline and would face less uplift.
The main one-off costs arise from assessing whether a facility, service or certification meets the revised pathways, registering newly captured assets and establishing a risk management program, and updating internal compliance processes to reflect the repeal of the customer-notification model. Newly captured

operators would also incur ongoing costs in maintaining that program and meeting annual reporting and incident reporting obligations. The measure may reduce regulatory cost for critical infrastructure customers that would no longer need to notify commercial providers under subsection 12F(3).

The measure is expected to have a limited effect on competition, innovation or market entry if the threshold is calibrated to capture significant facilities, larger Australian-facing service providers and certified hosting providers. Because a 1 MW threshold is low in industry terms, the principal impact question is whether it would draw in smaller providers, new entrants and operators situated close to the threshold. A higher threshold would narrow the affected population significantly.

Consultation questions

39. Is facility-based capture using rated IT load the right primary threshold for large, shared data-centre facilities? If so, is **1 MW** an appropriate threshold in the Australian market, and how should rated IT load be defined and measured?

40. For service-based capture, which Australian-facing metric or combination of metrics would best identify significant service-layer providers, such as revenue from in-scope services, customer or tenant numbers, data volume or employee headcount? How should the threshold avoid capturing smaller or incidental providers?

41. What aggregation rules are needed for campus-style or distributed data-centre operations so that integrated facilities are treated as one site where appropriate, without capturing unrelated facilities merely because they are co-located or commonly owned?

42. What service types should be expressly excluded from service-based capture, including pure software licensing, professional services, advisory services or incidental data handling? How should those exclusions be drawn?

43. How should possible reforms to the Hosting Certification Framework be taken into account in the proposed data storage or processing model, including the certification-based capture pathway and the existing exemption from CIRMP obligations for certain HCF-certified entities? For example, should any future HCF alignment be managed through amendments to existing SOCI exemption settings, the proposed general exemptions framework, service-based exemption arrangements, or direct application of Part 2A obligations with HCF addressing residual gaps?

Part B – Modernising and Refining Sector and Asset Coverage

Measure 9 – Space Technology

The problem

The SOCI Act already identifies a space technology sector, but no operative asset classes have been prescribed for that sector. As a result, the sector has no practical effect under the Act, and entities cannot assess whether SOCI obligations apply by reference to a dedicated space technology asset class.

Space-derived services now support multiple critical infrastructure sectors. Positioning, navigation and timing services, earth observation, space situational awareness, space-enabled communications and related data services can be important to communications, energy, transport, financial services, emergency management and other nationally significant activities.

The concern is that critical infrastructure and Government functions increasingly depend on ground-based and associated terrestrial systems in Australia that support, control, process or distribute space-derived services. If those systems are disrupted, degraded or compromised, the consequences may extend beyond the immediate operator and affect other critical infrastructure or Government functions.

Some space-related infrastructure may already be captured incidentally under other SOCI asset classes, particularly telecommunications or data storage or processing. Incidental capture can leave uncertainty about which function is being regulated, which entity is responsible, and whether the relevant risk is being managed because of the asset's telecommunications role, data role, or role in supporting a nationally significant space-derived service.

These issues make it difficult for industry to identify when space-related infrastructure is regulated under SOCI, why it is regulated, and which entity is responsible for managing the relevant security and resilience risk.

Proposed model for consultation: Establish four asset classes under the existing space technology sector to capture nationally significant ground-based and associated terrestrial systems in Australia. The four proposed asset classes are:

- ground segment infrastructure
- positioning, navigation and timing support infrastructure
- earth observation data infrastructure; and
- space situational awareness infrastructure.

The Act would establish the four asset-class categories. The Rules would prescribe the operative thresholds, technical boundaries, specified assets, requirements and exclusions for each category following further consultation.

The Rules could identify critical space technology assets by specifying particular assets, systems or facilities, or by prescribing requirements that an asset, system or facility must meet.

Rules consultation would focus on objective and administrable capture criteria. Potential criteria could

include the function performed by the system, the type of space-derived service supported, whether the system supports a prescribed class of critical infrastructure sector or Government function, whether the system forms part of a prescribed national capability or Government service arrangement, the scale or coverage of the service, the concentration or substitutability of the capability, and the role of the system in maintaining availability, integrity, reliability or security of the relevant service.

Space-related infrastructure would be assessed by reference to the asset class it falls within and the Rules-prescribed requirements that apply to that class. Ordinary commercial space activity, research activity, advisory services, incidental data handling, general analytics, ordinary automation and infrastructure with only a remote or ancillary connection to a space-derived service would remain outside scope unless a defined statutory pathway is met.

A limited reserve pathway is also being considered for certain Australian-registered, Australian-licensed or Australian-supervised satellites and other orbital assets. The pathway would be available only where capture is legally permissible and the asset is specified in the Rules or meets Rules-prescribed requirements. The current treatment of Commonwealth-owned assets is not proposed to change.

Matters for subsequent Rules consultation

The operative thresholds for each asset class would be developed through subsequent consultation on amendments to the Definitions Rules. The Department is seeking preliminary views on objective criteria that could identify nationally significant systems, such as:

- technical characteristics, including antenna capability, sensor capability, timing accuracy, processing capability, coverage area, data volume or operational availability
- scale of operation, including the number or class of satellites, space objects, reference stations, sensors, users, subscribers, customers or regulated entities supported
- formal service arrangements, including prescribed Government contracts, licences, authorisations, standing arrangements, service-level arrangements, accreditations or certifications
- service reach and substitutability, including geographic coverage, sectoral coverage, concentration of capability, availability requirements, redundancy, restoration timeframes or the availability of practical substitutes; and/or
- prescribed user or function classes, including Government entities, emergency services, responsible entities for critical infrastructure assets, regulated market operators or providers of essential services.

Rules consultation would also consider exclusions for systems whose connection to a space-derived service is remote, ancillary or incidental, and for systems whose disruption would have only localised or readily substitutable effects.

Key design elements

Element	Description
Ground-based and terrestrial focus	The reform would focus on ground-based space infrastructure and associated terrestrial systems physically located in Australia. This would provide a workable

Element	Description
	domestic regulatory basis and focus the measure on systems that perform operational, control, processing, distribution or assurance functions.
Ground segment infrastructure	This asset class would cover terrestrial systems in Australia used for command, control, telemetry, tracking, uplink, downlink, data reception, mission operations, tasking, scheduling, network management or associated operational support for satellite systems.
Positioning, navigation and timing support infrastructure	This asset class would cover terrestrial systems in Australia that support the reliability, integrity, correction, augmentation, authentication or distribution of space-derived positioning, navigation and timing services.
Earth observation data infrastructure	This asset class would cover terrestrial systems in Australia used for the reception, processing, storage, tasking or dissemination of satellite-derived earth observation data.
Space situational awareness infrastructure	This asset class would cover terrestrial systems in Australia used for monitoring, tracking, characterisation, space weather monitoring or associated processing functions.
Associated data processing and control functions	Associated data processing, control, tasking, scheduling, mission operations and AI-enabled functions could be captured where they form part of a proposed asset class and meet Rules-prescribed requirements. Rules consultation would consider boundaries for incidental data handling, general analytics and ordinary automation.
Orbital reserve pathway	A limited reserve pathway is being considered for certain Australian-registered, Australian-licensed or Australian-supervised satellites and other orbital assets. The pathway would be available where capture is legally permissible and the asset is specified in the Rules or meets Rules-prescribed requirements.
Overlap with telecommunications and data storage	The Rules and proposed exemptions framework would manage overlap with telecommunications and data storage or processing frameworks. Rules settings, exclusions or exemptions could address cases where the same function, system or capability is already adequately regulated elsewhere.
Responsible entity	The responsible entity would generally be the person that owns or operates the relevant asset. Where ownership, operation and control are split between entities, the model would focus on the entity best placed to manage the relevant security and resilience risk. For any orbital asset captured through a reserve pathway, the responsible entity would be the entity that holds the relevant permit or authorisation under the *Space (Launches and Returns) Act 2018*, or the entity that exercises effective operational control over the satellite.
Government-related services and	The current treatment of Commonwealth-owned assets is not proposed to change. Non-Commonwealth infrastructure could be considered where it supports Government functions or critical infrastructure sectors and otherwise meets the relevant statutory tests. Privately operated infrastructure supplied

Element	Description
Commonwealth-owned assets	under Government service contracts could be considered where the operator provides the relevant service on a commercial basis and the Rules-prescribed requirements are met.
Exclusions and boundaries	Space-related infrastructure would be assessed by reference to the function performed by the system, its connection to one of the proposed asset classes, and the Rules-prescribed requirements for that class. Ordinary commercial space activity, research activity, advisory services, incidental data handling, general analytics, ordinary automation and infrastructure with only a remote or ancillary connection to a space-derived service would remain outside scope unless a defined statutory pathway is met.
What is not changing	The current treatment of Commonwealth-owned assets would continue. Orbital assets would enter scope only through a limited reserve pathway where capture is legally permissible and the Rules specify the asset or prescribe requirements that the asset meets. Ordinary commercial space activity, research activity, advisory services and infrastructure with only a remote or ancillary connection to a space-derived service would remain outside scope unless a defined statutory pathway is met.

Preliminary Impact Analysis

This measure would give the existing space technology sector practical effect for the first time. It would do this through four bounded asset classes for ground segment infrastructure, positioning, navigation and timing support infrastructure, earth observation data infrastructure, and space situational awareness infrastructure located in Australia.

The affected population is modest and identifiable. It includes major commercial satellite gateways and teleports, tracking, telemetry and control facilities, reference and augmentation stations, and earth observation downlink and processing sites, with the most critical facilities operated by a small number of entities. Commonwealth-owned assets would retain their current treatment and remain outside scope, although privately operated infrastructure that serves Government on a commercial basis could be captured. A separate and deliberately limited orbital reserve pathway could capture a small number of Australian-registered, licensed or supervised satellite operators, but only where the Rules specify the asset or it meets prescribed requirements.

The expected costs for newly captured entities would be both one-off and ongoing. One-off costs would arise from assessing whether a system is captured, registering it, and establishing a risk management program (if applicable). Ongoing costs would arise from maintaining that program and meeting reporting obligations. Because some space infrastructure is already captured incidentally under the telecommunications or data storage classes, the dedicated asset classes would also clarify which function and which entity is regulated, removing a current source of uncertainty. Where capture would overlap those existing classes, the Rules and the exemptions framework are intended to resolve the overlap, so that the same capability is not regulated twice. Several significant ground stations already operate under security or accreditation requirements, so for those entities the measure would build on existing controls rather than require new arrangements.

The sector is emerging, so the effect on competition and innovation would depend on the final Rules-level thresholds. The proposed asset classes are limited to nationally significant ground-based systems, and ordinary commercial space activity, research activity, advisory services and general analytics would remain outside scope unless a defined statutory pathway is met. This should limit the burden on early-stage, research and specialised providers. The impact would depend more on the Rules-level thresholds and specified assets than on the Act-level asset classes themselves.

Consultation questions

44. Are the four proposed asset classes the right initial basis for giving operative effect to the existing space technology sector: ground segment infrastructure, positioning, navigation and timing support infrastructure, earth observation data infrastructure, and space situational awareness infrastructure? Should any class be narrowed, removed or supplemented?

45. Should the Act establish the proposed asset-class categories, with the operative thresholds, specified assets, requirements, technical boundaries and exclusions prescribed in the Rules following further consultation?

46. What objective Rules-level criteria would help entities assess whether a system within one of the proposed asset classes should be captured? Please comment on technical characteristics, scale of operation, formal service arrangements, service reach, substitutability, availability requirements, restoration timeframes, prescribed user or function classes, and any asset-class-specific criteria.

47. How should the framework manage associated data processing, control, tasking, scheduling, mission operations or AI-enabled functions where they form part of a proposed asset class? What boundaries are needed for incidental data handling, general analytics and ordinary automation?

48. Should the Act include a limited reserve pathway for certain Australian-registered, Australian-licensed or Australian-supervised satellites and other orbital assets, with capture depending on Rules prescription or Rules-prescribed requirements?

Measure 10 – Health Care and Medical Sector

The problem

The current SOCI framework reaches only part of the health care and medical sector's most significant infrastructure. It captures critical hospitals, but CIRMP obligations apply only to a designated subset of those hospitals. The framework also does not clearly capture other concentrated health and medical functions whose disruption, compromise or misuse could affect more than a single provider, facility or local service. This creates a gap between current SOCI coverage and the health functions most important to essential clinical services, public health capability, national security, and Australia's social and economic stability.

Health care and medical infrastructure is essential and highly exposed

Health care infrastructure is essential and highly exposed to contemporary threats. Disruption can affect patient safety, emergency care, elective care, public health response and confidence in the health system. ASD's *2024–25 Annual Cyber Threat Report* identifies that disruption of Australian healthcare networks can endanger patients, making the sector vulnerable to extortion by cybercriminals. The Report indicates that

ransomware incidents against the healthcare sector doubled in 2024–25 compared with 2023–24, and that malicious cyber actors were successful in 95 per cent of health care and social assistance sector incidents responded to by ASD's ACSC, compared with approximately 52 per cent across all sectors.

Critical hospital coverage is incomplete

The current hospital settings do not align well with how risk is governed across hospital networks, public health services and private hospital operators. Key cyber, personnel, supply chain, physical security and governance controls are often managed at network, health-service or corporate-operator level. Applying CIRMP obligations only to a designated subset of critical hospitals can create unnecessary complexity for operators that manage a shared control environment across multiple hospitals.

Concentrated blood supply functions are not clearly captured

The framework does not adequately address concentrated blood supply functions. Blood and blood products support emergency treatment, trauma care, surgery, obstetrics, cancer treatment and ongoing care for patients with chronic or rare conditions. These functions are time-sensitive, clinically essential and difficult to substitute at short notice. Disruption to testing, processing, storage, component manufacture, fractionation, distribution or access to clinically essential products can affect multiple hospitals and clinical settings.

The concern for SOCI is concentrated blood supply functions where limited substitutes, or dependence on a small number of providers or supply arrangements, could create broader health-system consequences.

Integrated pathology systems can have system-wide consequences

Pathology is embedded in ordinary clinical decision-making and public health response. Diagnostic testing, blood matching, infectious disease testing and specialised laboratory services are essential to emergency care, inpatient care, elective care, primary care and public health surveillance. Large integrated pathology systems can support multiple hospitals, clinicians and jurisdictions. Disruption to those systems can quickly affect clinical workflows, delay diagnosis and treatment, and reduce public health situational awareness.

The concern for SOCI is integrated pathology capability operating at a scale where disruption could produce consequences across the health system.

High-containment and specialised laboratories present distinct risks

There is also a gap in how the framework deals with high-containment and specialised laboratory capability. Some laboratory facilities perform functions that are material to public health, biosecurity, national security or high-consequence human, zoonotic or animal disease response. This may include facilities handling Security Sensitive Biological Agents, Physical Containment Level 3 (PC3) and Level 4 (PC4) facilities, and specialised laboratories that support detection, diagnosis, characterisation or response for high-consequence pathogens or diseases. The risk profile extends beyond service interruption. Disruption, compromise or misuse of these capabilities may affect public health preparedness, biosecurity response, sensitive biological material security, confidence in disease response systems, or the continuity of functions that support national security and economic stability.

Existing health, accreditation and biosecurity frameworks remain important

Existing sectoral regulation addresses important matters such as clinical safety, accreditation, therapeutics, public health and biosecurity. Those frameworks regulate safety, quality, clinical, therapeutic, public health and biosecurity matters. The gap for SOCI is different. It relates to national visibility, governance, all-hazards risk management, assurance, incident response and continuity for health and medical functions whose

disruption, compromise or misuse could affect essential services, public confidence, national security, public health capability, or Australia's social and economic stability.

The policy problem is a targeted coverage gap for health and medical functions that may create broader consequences because of their criticality, concentration, dependence, time sensitivity, limited substitutability, containment risk or shared operational control. The current framework does not consistently reach those functions or provide a clear way to manage their interaction with existing health, therapeutic goods, laboratory accreditation, public health, biosecurity and SSBA frameworks.

Case study: Synnovis ransomware attack, United Kingdom

In June 2024, Synnovis, a pathology provider to the United Kingdom's National Health Service, was affected by a ransomware attack that disrupted diagnostic, blood testing and pathology services across hospitals, general practices and other healthcare providers in south-east London.

The disruption affected core clinical workflows almost immediately. Seven hospitals were affected, with 1,134 planned operations and 2,194 outpatient appointments cancelled in the first 13 days. Blood testing in London reportedly fell to around 10 per cent of normal levels, and more than 11,000 appointments were ultimately cancelled or delayed. The incident also disrupted blood testing and blood matching, contributing to pressure on blood stocks.

The attack also involved the theft and publication of sensitive patient data. A patient safety investigation into an unexpected patient death found that the cyber attack was a contributing factor, including because of a long wait for a blood test result while pathology services were disrupted. Nearly 600 incidents were linked to the attack, with patient care affected in 170 cases.

The incident illustrates why this measure is focused on large, integrated or systemically significant pathology functions, and other concentrated health and medical functions, where disruption can affect clinical continuity, patient safety, public confidence and health-system resilience beyond a single facility or local service.

Proposed model for consultation: Apply CIRMP obligations more consistently to critical hospitals, and create new asset classes for critical blood supply, critical pathology, and nationally significant high-containment or specialised laboratory capability. The new asset classes would focus on functions that are concentrated, systemically significant or otherwise material to national security or the social or economic stability of Australia or its people.

For critical hospitals, the proposed model would address the current split between critical hospitals that are captured under SOCI and the subset that is subject to CIRMP obligations. The objective is to better align risk-management obligations with how cyber, personnel, supply chain, physical security and governance controls are managed across hospital networks, public health services and private hospital operators.

The Department is considering new asset concepts for critical blood supply and large integrated pathology systems. The blood supply concept would be capable of addressing operational blood supply functions in Australia, including collection, testing, processing, storage, component manufacture, fractionation and distribution of critical blood and blood products. Capture would be informed by existing therapeutic goods regulation, including manufacturing licences under section 38 of the *Therapeutic Goods Act*, and scale thresholds prescribed in the Rules.

The pathology concept would focus on integrated systems of Accredited Pathology Laboratories operating at systemically significant scale. The Rules would prescribe the relevant scale threshold, including by reference to the number of Accredited Pathology Laboratories, the number of States and Territories in which the system operates, and the volume of testing episodes processed through the system.

A further proposed asset limb would address nationally significant high-containment or specialised laboratory capability. This could include prescribed PC3 or PC4 facilities, facilities handling SSBAs, and laboratory capability that is material to public health, biosecurity, national security or high-consequence human, zoonotic or animal disease response. The focus would be on facilities and capabilities whose disruption, compromise or misuse could have consequences beyond a single institution, local service or ordinary laboratory function.

Any expansion of coverage in the health care and medical sector is intended to be targeted, proportionate and aligned as far as possible with existing health, accreditation, therapeutic goods, public health, biosecurity, SSBA and laboratory regulatory frameworks. Further implementation and Rules consultation would address detailed thresholds, exclusions, equivalent-framework recognition and transition settings.

Key design elements

Element	Description
Critical blood supply	The proposed blood supply asset class would focus on operational blood supply functions in Australia. The asset would comprise one or more facilities and information systems used for collection of human blood or blood components, testing for transfusion safety or release for use, processing or manufacturing of human blood components, or fractionation of human plasma into plasma-derived therapeutic products, where those activities are concentrated and systemically significant. The Department is also considering whether critical blood product supply functions should be captured, including imported plasma-derived products such as immunoglobulin and clotting factor products, where limited substitutability and clinical dependence mean disruption could have broader health-system consequences.
Critical pathology	The proposed pathology asset class would apply to public, private or mixed pathology systems that operate at systemically significant scale. The asset class could comprise one or more Accredited Pathology Laboratories, laboratory information systems used in connection with those laboratories, specimen logistics infrastructure, and data holdings comprising pathology results and associated patient information generated by those laboratories. The Rules would prescribe the relevant criticality thresholds, system boundaries and exclusions, including by reference to testing volume, integration, geographic reach, market concentration, specialised capability, clinical dependency and substitutability.

Element	Description
High-containment and specialised laboratory capability	The Department is seeking views on whether a further asset limb should address nationally significant laboratory facilities or capabilities where disruption, compromise or misuse could have material public health, biosecurity, national security or economic consequences. The Rules could prescribe relevant facility types, capability thresholds and exclusions. This may include PC3 or PC4 facilities handling Security Sensitive Biological Agents, and laboratories supporting high-consequence human, zoonotic or animal disease detection, diagnosis, characterisation or response. The limb would not be limited to human health laboratories where an animal health, biosecurity or public health surge capability performs an equivalent nationally significant function.
Exclusions and proportionality	The reform would apply only to prescribed health and medical functions that meet the relevant statutory pathway and Rules-prescribed thresholds. Rules consultation would consider exclusions for arrangements that do not give rise to comparable system-level dependence or national consequence, including ordinary pharmacy activity, ordinary home delivery arrangements, point-of-care testing, research-only activity, local pathology services, individual laboratories operating below the relevant threshold, hospital transfusion services and hospital blood banks. Ordinary veterinary pathology and forensic pathology would remain outside scope unless the relevant facility or capability meets a defined high-containment, public health, biosecurity or specialised laboratory pathway.
What is not changing	The reform would not regulate ordinary health care and medical activity. Individual donors, patients, ordinary pharmacies, ordinary home delivery arrangements, non-critical pathology services, individual laboratories, hospital blood banks and point-of-care testing would remain outside scope unless a defined statutory pathway and Rules-prescribed threshold are met.

Preliminary Impact Analysis

This measure is likely to bring additional health care and medical entities within SOCI where they operate systemically significant functions. The impact would be uneven because parts of the sector are highly concentrated. Of Australia's approximately 700 public hospitals, most are small, and only the large tertiary facilities would meet a critical-hospital threshold. Private pathology is more concentrated, with three providers holding more than 80 per cent of approved collection centres. The blood supply is more concentrated again, with a single national supplier of fresh blood products and a single domestic manufacturer of fractionated plasma products. High-containment laboratory capability is held in a small number of PC4 facilities, almost all of which are public or research institutions. The number of entities newly in scope would therefore be small, although several are individually critical.

For newly captured entities, the expected costs would be both one-off and ongoing. One-off costs arise from assessing whether a function meets the relevant threshold, registering captured assets, developing

or extending CIRMP arrangements, and aligning SOCI obligations with existing health, therapeutic goods, laboratory-accreditation, public health, biosecurity and SSBA frameworks. Ongoing costs arise from maintaining the CIRMP and meeting annual reporting and incident reporting obligations. Because pathology, blood and high-containment functions are concentrated in a small number of large, well-resourced organisations that already maintain mature security and quality systems, the incremental cost in those functions is expected to be manageable.

The measure is expected to have a limited effect on competition, innovation or market entry where thresholds are calibrated to capture only concentrated or systemically significant functions. The principal driver of impact is the boundary: where the critical-hospital threshold is set, and whether the pathology and laboratory thresholds capture smaller or regional providers and specialised laboratories alongside the major operators.

Consultation questions

49. What scale thresholds should apply to critical blood supply functions, including collection, testing, processing, manufacture and fractionation? What exclusions should apply for National Blood Authority coordination systems, hospital transfusion services, hospital blood banks, clinical trials, autologous or directed donation services, and research-only collections?

50. For the proposed critical pathology asset class, are Accredited Pathology Laboratories, common ownership or control, States and Territories of operation, and annual testing episodes appropriate objective markers for identifying integrated pathology systems operating at systemically significant scale?

51. Should a further asset limb address nationally significant high-containment or specialised laboratory capability? If so, what prescribed facility types, capability thresholds and exclusions should be considered?

52. How should SOCI settings interact with existing health, therapeutic goods, laboratory accreditation, public health, biosecurity, SSBA and Commonwealth protective security frameworks, including through Rules settings, transition arrangements and the proposed exemptions framework?

Measure 11 – Distributed Energy Resources

The problem

The current electricity framework in the SOCI Act was developed around a more centralised, site-based model of generation, transmission and distribution. It does not deal clearly with newer distributed energy resource models, where electricity-system significance may come from storage, controllable demand, demand-response capability, or the coordinated operation of many smaller assets.

This creates uncertainty for industry because the current framework relies on concepts that are closely associated with conventional generation stations and network assets. The status of electricity storage systems, including battery energy storage systems, is not clear enough under the current generation-focused framework. This can make it difficult for storage operators to assess whether SOCI obligations apply.

The current model also does not clearly accommodate virtual power plants, DER aggregation, demand-response aggregation and other software-enabled control models. In those arrangements, the relevant operational capability may sit with the person that has contractual or technical ability to direct, coordinate, dispatch, orchestrate or materially influence the operation of a portfolio.

Portfolios of smaller assets can also remain outside scope even where their combined capacity, coordinated operation or dispatch capability is comparable to a larger concentrated generation or storage asset. For example, multiple smaller assets under common operation, dispatch control or orchestration control may have electricity-system consequences comparable to a single larger asset.

These issues make it difficult for industry to know when storage, controllable demand, aggregation, orchestration or dispatch arrangements are important enough to be regulated under SOCI, and which entity should be responsible where control is exercised through software, contracts or portfolio arrangements.

Distributed energy resources are used in this measure to refer to electricity resources, devices, systems and portfolios that can generate, store, consume, reduce or shift electricity demand, or be coordinated to provide electricity system services. This may include distributed generation, electricity storage, controllable demand, demand-response capable assets and the platforms or arrangements used to aggregate, orchestrate or dispatch them.

Proposed model for consultation: Update the critical electricity asset framework so it can more clearly address four functional categories of DER: distributed generation, distributed storage, controllable demand or demand-response capable assets, and aggregation, orchestration or dispatch platforms.

The Act would provide a clearer enabling basis for electricity storage systems, including battery energy storage systems (BESS), and for aggregation, orchestration or dispatch arrangements where system significance arises from coordinated control of distributed generation, storage or controllable demand assets.

The reform would preserve the existing threshold-based model. The Rules would continue to prescribe the detailed requirements for when an asset, portfolio, platform or arrangement is critical. Rules consultation would consider capacity metrics, aggregation rules, market definitions, common-control concepts, dispatch or orchestration control, geographic or market concentration, and exclusions for low-consequence arrangements.

A coordinated portfolio, aggregation arrangement or orchestration system could itself be the relevant critical asset where prescribed thresholds are met. Thresholds could be based on matters such as registered capacity, nameplate capacity, dispatchable capacity, aggregated controllable capacity, maximum demand, contracted capacity, metered load, market participation, number of controlled devices, common operation or control, and practical ability to coordinate dispatch or operation at scale.

The responsible entity would generally be the person with substantive contractual or technical ability to direct, coordinate, dispatch, orchestrate or materially influence the operation of the in-scope asset, portfolio, platform or arrangement.

Regulated status would be confined to assets, portfolios, platforms or arrangements that meet a defined statutory pathway and Rules-prescribed threshold. Small standalone consumer assets, household batteries, rooftop solar installations, ordinary demand-response capable appliances, ordinary electricity consumption, installation services, retail contracting, equipment manufacture, software support and

platform provision without substantive operational, dispatch or orchestration control would remain outside scope.

Key design elements

Element	Description
DER functional categories	The Act would recognise four functional categories: distributed generation, distributed storage, controllable demand or demand-response capable assets, and aggregation, orchestration or dispatch platforms. Detailed thresholds, exclusions, asset boundaries and sector-specific application settings would be prescribed in the Rules.
Electricity storage	The framework would expressly recognise electricity storage systems, including BESS, within the critical electricity asset settings. This would provide a clearer basis for storage operators to assess whether SOCI obligations may apply. The Rules would prescribe when an electricity storage system is critical. Rules consultation could consider capacity metrics such as registered capacity, nameplate capacity, dispatchable capacity or another prescribed capacity measure. Grid-scale or utility-scale storage could be treated directly where it meets the relevant threshold. Household or behind-the-meter batteries would generally be relevant only where aggregated, orchestrated or dispatched as part of an in-scope portfolio.
Aggregation, orchestration and dispatch	The framework would recognise coordinated control, dispatch or orchestration of multiple distributed generation, storage or controllable demand assets, including virtual power plants, DER aggregation and demand-response aggregation models. This would include arrangements where a person can issue control signals, optimise dispatch, curtail output, charge or discharge storage, coordinate demand response, or materially influence operation of a DER portfolio. A software or platform provider would be relevant where it has substantive technical or contractual ability to direct, coordinate, dispatch, orchestrate or materially influence portfolio operation. Software supply, hosting or support without that substantive control would remain outside scope.
Portfolio aggregation	A coordinated portfolio, aggregation arrangement or orchestration system could be treated as the relevant critical asset where prescribed aggregation criteria are met. Rules consultation would consider how aggregate capacity should be calculated across assets under common operation, dispatch control, contractual control, market participation responsibility or orchestration control. Potential threshold metrics could include registered capacity, nameplate capacity, dispatchable capacity, aggregated controllable capacity, number of controlled devices, market participation and geographic or network concentration.

Element	Description
Controllable demand and flexible load	Large flexible loads, including industrial loads, may be relevant where they meet prescribed thresholds or are coordinated through an aggregation or demand-response arrangement. Rules consultation could consider thresholds based on maximum demand, contracted capacity, metered load, dispatchable demand response, market participation or connection to a prescribed class of strategic or industrial load. Ordinary electricity consumption and ordinary demand-response capability would remain outside scope.
Multi-touchpoint dependencies	DER risks can arise through several operational touchpoints, including device owners, manufacturers, firmware providers, software platforms, cloud services, installers, aggregators, orchestrators, retailers, original equipment manufacturers and offshore support arrangements. The framework would not treat every participant in the DER environment as a responsible entity. The Rules and guidance would identify which roles are relevant to asset capture, registration, risk management, and supplier assurance. Capture would focus on substantive operational, dispatch or orchestration control.
Thresholds	The reform would retain a threshold-based regime. The Act and Rules would provide clearer concepts for storage, controllable demand, common operation or control, capacity metrics and wholesale market settings. Rules consultation would consider threshold metrics for different DER functions, including registered capacity, nameplate capacity, dispatchable capacity, aggregated controllable capacity, maximum demand, contracted capacity, metered load, market participation, number of controlled devices, geographic concentration, wholesale market participation, and practical ability to coordinate operation at scale.
Exclusions and proportionality	The reform would avoid capturing low-consequence DER activity. Small standalone consumer assets would remain outside scope where they only generate, store or consume electricity, or participate in demand response. Ordinary device ownership, installation, retail contracting, software support, equipment manufacture and platform provision would also remain outside scope unless they involve substantive operational, dispatch or orchestration control. Capture would turn on substantive operational, dispatch or orchestration control, or another defined statutory pathway. A small or medium entity would only be captured where its role, access, control or coordinated portfolio scale meets Rules-prescribed thresholds. Rules consultation would consider exclusions and modified compliance approaches for small portfolios, low-impact arrangements and participants whose role is incidental or adequately managed through a responsible entity's CIRMP, supplier assurance or relevant operator arrangements.

Element	Description
Responsible entity	The responsible entity would generally be the person with substantive contractual or technical ability to direct, coordinate, dispatch, orchestrate or materially influence an in-scope asset, portfolio or platform. Virtual power plant operators, DER aggregators or demand-response aggregators may often be the relevant entity. Retailers, original equipment manufacturers, software providers or platform operators would be relevant only where they hold substantive operational, dispatch or orchestration control.
What is not changing	The existing critical electricity asset framework would remain the foundation of the reform. The reform would modernise that framework so it can deal more clearly with storage, aggregation, controllable demand and portfolio-based system significance. The reform would preserve a threshold-based approach and rely on the Rules to calibrate asset boundaries, metrics, exclusions and transition settings. Regulated status would be confined to assets, portfolios, platforms or arrangements that meet a defined statutory pathway and Rules-prescribed threshold.

Preliminary Impact Analysis

This measure is likely to result in additional electricity-sector entities becoming subject to SOCI obligations where they exercise material operational, dispatch or orchestration control over electricity storage, controllable demand or aggregated DER portfolios. The measure is directed at aggregators and orchestrators, rather than households or individual asset owners. The number of affected entities would depend on the aggregated capacity or degree of control at which the threshold is set.

The expected costs would comprise both one-off transition costs and ongoing compliance costs. One-off costs arise from the threshold assessment, registration, and mapping the entity's operational control, supplier dependencies and remote-access arrangements. Captured entities would then incur ongoing CIRMP and reporting obligations. Because orchestration depends on software platforms and remote access, the cyber and supply-chain elements of any CIRMP obligation are expected to be the main source of compliance effort. The aggregator and virtual power plant market is still developing, so some affected entities, including smaller aggregators, would be subject to security obligations for the first time.

The effect on competition, innovation and market entry would depend on threshold settings, particularly because the market is still developing. Thresholds calibrated to genuine systemic control would leave scope for new entrants, whereas lower thresholds could impose obligations on early-stage operators before they reach scale.

Consultation questions

53. Is the proposed four-category DER model the right Act-level architecture for distributed generation, distributed storage, controllable demand or demand-response capable assets, and aggregation, orchestration or dispatch platforms?

54. What Rules-level thresholds would best distinguish systemically significant storage assets, DER portfolios, aggregation arrangements and orchestration platforms from small standalone consumer assets or lower-consequence arrangements? Please comment on registered capacity, nameplate capacity, dispatchable capacity, aggregated controllable capacity, maximum demand, contracted capacity, metered load, market participation, number of controlled devices and geographic concentration.

55. How should the framework identify common operation or control for portfolio aggregation? Please comment on ownership, operation, dispatch control, contractual control, market participation responsibility, orchestration rights, remote access arrangements and practical ability to coordinate operation at scale.

56. Should the responsible entity generally be the person with substantive contractual or technical ability to direct, coordinate, dispatch, orchestrate or materially influence operation of an in-scope asset, portfolio, platform or arrangement? What role-based boundaries are needed for retailers, original equipment manufacturers, software providers or platform operators?

57. What exclusions, modified compliance approaches or guidance would help avoid capture of low-consequence DER activity, including small standalone consumer assets, ordinary device ownership, installation, retail contracting, software support, equipment manufacture or incidental platform services?

58. Should smart metering systems, advanced metering infrastructure, meter data platforms or associated cloud-based control and analytics systems be capable of capture where they provide remote access, operational visibility, control, orchestration, demand response, network-management or system-security functions at material scale? What thresholds and role-based boundaries would distinguish those systems from ordinary metering, billing or customer-service functions?

Measure 12 – Offshore Electricity Assets

The problem

The SOCI Act currently limits capture by reference to asset location. As a result, electricity infrastructure located beyond the territorial sea can fall outside the SOCI framework even where it is regulated under the Commonwealth offshore electricity regime and may become important to electricity system security or reliability.

This creates a foreseeable coverage gap as offshore electricity projects move from feasibility and development into operation. The issue is most likely to arise in Commonwealth offshore areas where Australia regulates offshore electricity infrastructure, but the current SOCI location settings may still prevent capture. Offshore wind is the clearest current example, although the issue could apply to offshore electricity infrastructure more generally. The result is that nationally significant offshore electricity infrastructure may

sit outside SOCI even where it forms part of Australia's energy system, is subject to Australian regulatory oversight, and would otherwise meet the relevant critical electricity asset thresholds.

Proposed model for consultation: Disapply the current geographic limitation for critical electricity assets located in Commonwealth offshore areas, so that offshore electricity infrastructure can be considered under the SOCI framework where it otherwise meets the relevant Act and Rules thresholds.

The proposal is intended to be technology-neutral and would apply to critical electricity assets in Commonwealth offshore areas generally. This could include offshore wind generation assets, associated subsea electricity cables, offshore substations, connection infrastructure and other enabling or supporting offshore electricity infrastructure, as well as other offshore electricity technologies that may emerge over time.

The reform would use the concept of Commonwealth offshore area from the *Offshore Electricity Infrastructure Act 2021*. This would align SOCI's geographic reach with areas where Australia exercises recognised sovereign rights and regulatory control for offshore electricity infrastructure.

The ordinary SOCI framework would continue to apply. An offshore electricity asset would still need to meet the relevant critical electricity asset definition and Rules thresholds before SOCI obligations apply. The reform would remove the location-based barrier, not change the underlying criticality test.

Key design elements

Element	Description
Commonwealth offshore areas	The reform would apply to critical electricity assets located in Commonwealth offshore areas, using the concept of Commonwealth offshore area from the *Offshore Electricity Infrastructure Act 2021*. This would align the SOCI framework with areas where Australia exercises recognised sovereign rights and regulatory control for offshore electricity infrastructure.
Technology-neutral approach	The proposal would apply to critical electricity assets in Commonwealth offshore areas generally, including offshore wind and other forms of offshore electricity infrastructure that may emerge over time.
Existing thresholds preserved	The reform would remove the current location-based barrier. The asset would still need to meet the relevant critical electricity asset definition and Rules thresholds to fall within scope.
Ordinary SOCI framework applies	If an offshore electricity asset falls within scope, it would be regulated through the existing SOCI architecture. The ordinary critical electricity asset obligations would apply, including responsible entity settings, registration, reporting, incident notification and risk management requirements.

Preliminary Impact Analysis

This measure is likely to result in some offshore electricity assets becoming subject to SOCI obligations where they are located in Commonwealth offshore areas and otherwise meet the existing critical electricity asset thresholds. The near-term population is very small. Australia has six declared offshore wind areas and approximately a dozen feasibility licences, and no offshore generation asset is yet operational. Capture would begin only as projects move from development into operation, which is several years away for most proponents.

Costs would arise at the operational stage and would include both one-off and ongoing elements. One-off costs would include threshold assessment, registration, and alignment with offshore electricity licensing and the project's ownership, operation and maintenance arrangements. Once an asset is captured, the proponent would incur ongoing CIRMP and reporting obligations. Because most projects are several years from operation, proponents would have time to plan for compliance, limiting transitional cost. The measure is expected to have little effect on competition or market entry because it would not create a separate offshore electricity regime or change the underlying criticality thresholds. The affected proponents are also few and already engaged with a dedicated Commonwealth licensing framework.

Consultation questions

59. Should the geographic exception apply to critical electricity assets generally in Commonwealth offshore areas, using the *Offshore Electricity Infrastructure Act 2021* concept of Commonwealth offshore area?

60. Are there practical or jurisdictional issues in applying ordinary SOCI obligations to offshore electricity assets in Commonwealth offshore areas, including issues relating to ownership, operation, maintenance, control or responsible entity identification?

61. What transition issues should be taken into account as offshore projects move from feasibility and development into operation and become capable of meeting the relevant critical electricity asset thresholds?

Measure 13 – Critical Freight

The problem

The current freight framework is narrow, geographically constrained and difficult to apply to modern freight dependencies. It relies on a closed list of asset types and does not deal well with freight nodes, chokepoints, logistics systems, distribution facilities or other dependencies whose disruption could have broader supply-chain or national resilience consequences. It can also miss important intrastate freight dependencies where the consequences of disruption are significant, even where the asset does not fit the current interstate framing.

Modern freight criticality may arise from concentration, operational interdependence, limited substitutability or a single point of failure. A transfer node, intermodal interface, distribution facility, cold chain facility, freight-management platform, operational control system or discrete chokepoint may be significant because disruption would affect the movement of goods beyond the immediate site or operator.

The current freight-services model also does not identify the regulated asset boundary clearly enough. Section 12C refers to the "network" used by a freight business. In practice, that concept can point either to the entity's own systems and facilities or to public infrastructure on which the entity depends. This makes the framework harder for freight businesses to apply and can misalign obligations with the parts of the freight operation that the entity can manage, secure and assure.

Connected road transport systems may also become relevant where they monitor, control or manage transport operations at significant scale. These systems are not freight assets in the ordinary sense, although compromise, degradation or unavailability of some systems could affect freight continuity, transport safety, defence, national security, the security or resilience of another critical infrastructure sector, or broader transport operations.

Together, these issues can make it unclear which freight assets are nationally significant, which parts of a freight business are regulated, and how the framework should deal with shared or connected transport systems. They can also leave important supply-chain dependencies outside SOCI where their disruption could have consequences beyond a single site, operator or jurisdiction.

Proposed model for consultation: Broaden and refine the freight framework so it can better identify nationally significant freight dependencies and clarify the asset boundary for freight service businesses. The reform proposes three key changes:

- First, the Act would provide an enabling basis for a broader range of nationally significant freight infrastructure assets by setting out the freight-related asset types that may be capable of capture. These could include freight nodes, intermodal interfaces, transfer points, port-to-distribution interfaces, distribution nodes, cold chain facilities, freight logistics platforms, operational technology systems and discrete chokepoints. The Rules would determine operative capture within those Act-level asset types by prescribing specified assets or entities, prescribing threshold criteria for broader classes of asset or entity, and prescribing exclusions where appropriate. This would allow nationally significant freight dependencies, including important intrastate dependencies, to be considered where they meet Rules-level thresholds.
- Secondly, the Act would clarify the freight-services asset boundary. For a critical freight business, the regulated asset would be the systems, facilities and operational capabilities that the business owns, operates or controls in carrying on the freight service. This may include terminals, depots, yards, control centres, dispatch systems, cargo management systems, fleet control systems, scheduling systems, operational communications, logistics platforms, operational technology systems, information technology systems and data holdings. Public infrastructure that the business merely uses would generally remain outside the freight-services asset boundary unless that infrastructure is separately captured through a defined statutory pathway.
- Thirdly, the Department is seeking views on whether a targeted connected transport systems pathway should be included. Such a pathway could apply to systems used to monitor, control or manage traffic or transport operations at significant scale. Examples may include traffic management centres, smart motorway control systems, adaptive traffic control systems, cooperative intelligent transport systems, electronic tolling systems, connected vehicle trust frameworks and large-scale operational technology systems. The Department is seeking views on whether these systems should be capable of capture under SOCI, whether they should be addressed within the freight framework

or a distinct but related asset concept, and what thresholds, safeguards, exclusions and intergovernmental arrangements would be needed.

The Act would establish the enabling concepts, asset-boundary principles and capture pathways. The Rules would identify the relevant thresholds and exclusions, so the framework can distinguish nationally significant freight dependencies from local or lower-consequence operations.

The reform is not intended to regulate all freight, logistics or transport infrastructure. Ordinary warehouses, local depots, local roads, local traffic systems, individual vehicles, small fleet telematics, ordinary public infrastructure and lower-consequence logistics operations would remain outside scope unless they meet a defined statutory pathway and Rules-level threshold.

Key design elements

Element	Description
Broader freight perimeter	The Act would set out broader classes of freight-related assets that may be capable of capture where they are nationally significant. These could include freight nodes, intermodal interfaces, transfer points, port-to-distribution interfaces, distribution nodes, cold chain facilities, freight logistics platforms, operational technology systems and discrete chokepoints. The Rules would determine which assets are captured by prescribing specified assets or entities, threshold criteria and exclusions.
Nationally significant freight nodes and chokepoints	Freight nodes, intermodal interfaces, transfer points, distribution nodes, cold chain facilities, freight logistics platforms, operational technology systems, chokepoints or other concentrated dependencies could be captured where disruption could affect the movement of goods beyond the immediate site or operator. Examples could include a major intermodal terminal, a port-to-distribution interface, a concentrated multi-sector distribution node, a temperature-controlled storage or cold chain facility, or a discrete freight chokepoint such as a bridge, tunnel, overpass or corridor segment. These examples would not be captured automatically and would need to meet the relevant statutory pathway and Rules-level threshold.
Freight-services asset boundary	For a critical freight business, obligations would attach to the systems, facilities and operational capabilities the business uses to carry on the freight service. This would avoid relying on an uncertain “network” concept that may point to public infrastructure the business does not own or control. Relevant systems and capabilities could include terminals, depots, yards, control centres, dispatch systems, cargo management systems, fleet control systems, scheduling systems, operational communications, logistics platforms, operational technology systems, information technology systems, data holdings and other operational assets through which the freight task is carried on.

Element	Description
Entity-controlled operational capability	The framework would focus on the parts of the freight operation that the responsible entity can manage, secure and assure. Where a freight business depends on public infrastructure, the regulated freight-services asset would be the business's own systems, facilities and operational capabilities.
Connected road transport systems under consideration	The Department is seeking views on whether a targeted connected transport systems pathway should be included. Such a pathway could apply to a system, or network of systems, that monitors, controls or manages traffic or transport operations at significant scale. Examples that may warrant consideration include traffic management centres, smart motorway control systems, adaptive traffic control systems, cooperative intelligent transport systems, connected vehicle trust frameworks and large-scale operational technology systems used for lane control, ramp metering, variable speed limits, incident response or network operations. Where a connected transport system is owned or operated by a State or Territory government, detailed design would need to take account of existing State and Territory responsibilities for road operations, transport safety, cyber security and network management.
Consequence and Rules-based calibration	The Rules would set thresholds, identify prescribed asset kinds, prescribe exclusions and refine the concept of system significance. Relevant threshold criteria may include throughput, freight volume, revenue, geographic reach, market concentration, operational interdependence, limited substitutability, duration of likely disruption, role in essential or time-sensitive supply chains, and consequences for dependent sectors, communities, defence or national security. For any consequence-based pathway, consultation could consider whether an extended disruption should be assessed by reference to effects on freight services in regions above a prescribed population threshold, disruption to essential goods such as food, fuel, water treatment supplies, medical supplies or defence materiel, effects on other critical infrastructure assets, or effects on defence capability or national security.
Overlap and interaction with other frameworks	Some freight-related assets and systems may also be subject to transport safety, security, planning, road, rail, port, aviation, workplace safety or other regulatory frameworks. The proposed exemptions framework would be used to manage duplication where another framework delivers substantially equivalent or stronger outcomes. Rules consultation would also consider exclusions where the primary function of an asset is already captured under another SOCI asset class.
What is not changing	The reform is directed to nationally significant freight assets, services and supporting systems whose disruption would have broader supply-chain, resilience, defence or national security consequences. Ordinary freight, logistics and transport activity would remain outside scope unless a defined statutory pathway and Rules-level threshold are met. Ordinary warehouses, local depots, local roads, local traffic systems, individual vehicles,

Element	Description
	small fleet telematics, ordinary public infrastructure and lower-consequence logistics operations would remain outside scope.

Preliminary Impact Analysis

This measure is likely to bring additional freight and transport entities within SOCI where they own or operate nationally significant freight nodes, logistics systems, distribution facilities, chokepoints or connected transport systems that meet Rules-level thresholds. It would also clarify obligations for critical freight businesses by focusing the regulated asset on the systems and capabilities the business owns, operates or controls. In practice, the measure is directed at major ports, intermodal terminals, large distribution networks and operators of nationally significant supply-chain nodes.

The expected costs include one-off transition costs and ongoing compliance costs. One-off costs arise from threshold assessment, asset and systems mapping, registration, and alignment with existing transport safety, security, road, rail, port, aviation, workplace-safety and State or Territory regulatory frameworks. Captured entities would then incur ongoing CIRMP and reporting obligations. Entities that operate networks across several jurisdictions are likely to face the highest mapping and alignment costs, because freight networks frequently cross State and Territory borders.

The measure may affect medium and large operators, including some regional operators and operators of specialised supply-chain nodes. The effect on competition is expected to be limited if thresholds are calibrated to capture only nationally significant dependencies. The principal drivers of impact are the threshold settings and whether a connected transport systems pathway proceeds.

Consultation questions

62. Is the proposed model a workable Act-level basis for freight reform, covering nationally significant freight infrastructure assets, defined capture pathways, and entity-controlled freight systems and operational capabilities?

63. What Rules-level criteria should be used to distinguish nationally significant freight dependencies from local or lower-consequence facilities? Please comment on freight volume, throughput, revenue, substitutability, market concentration, geographic reach, role in time-sensitive or essential supply chains, and consequences for dependent sectors, communities, defence or national security.

64. Does the proposed freight-services asset boundary appropriately distinguish the systems, facilities and operational capabilities controlled by the freight business from public infrastructure the entity does not own or control?

65. Should connected transport systems be capable of capture where compromise, degradation or unavailability could materially affect freight continuity, transport safety, defence, national security, the security or resilience of another critical infrastructure sector, or broader transport operations at a nationally significant scale? If so, should that pathway sit within the freight framework or in a distinct but related asset concept, and what thresholds, exclusions or intergovernmental arrangements would be needed?

Measure 14 – Higher Education and Research

The problem

The current higher education and research framework is difficult for research entities to apply because it does not align well with the way nationally significant sensitive research is conducted in practice. The current definition is tied to an asset owned or operated by a university and used in connection with undertaking a program of research that is critical to another critical infrastructure sector, the defence of Australia or national security.

That model creates three practical issues:

- First, the current definition is limited to assets owned or operated by universities. Equivalent nationally significant research may be conducted by public research bodies, private research entities, commercial entities, cooperative research structures, joint ventures or other collaborative arrangements.
- Secondly, the concept of a program of research does not always align with how sensitive research is organised. Research of national significance may be conducted through a sustained research function, such as a facility, platform, laboratory, secure data environment, specialist centre or continuing research capability. These arrangements may support multiple projects over time without fitting neatly within a single program of research.
- Thirdly, the current "critical to" test can be difficult to apply consistently. It requires judgments about whether research is critical to another critical infrastructure sector, defence or national security, but provides no clear statutory method for making that judgment. This can make the boundary between in-scope and out-of-scope research uncertain for universities and other research entities.

These difficulties are more pronounced where research is conducted in advanced or dual-use fields. Research in fields such as artificial intelligence, quantum technologies, advanced materials, autonomous systems, biotechnology, cyber security and space-related capabilities may have legitimate civil, commercial and public-benefit applications while also carrying potential defence, intelligence, security or critical infrastructure implications. The Act should provide a clearer and more predictable way to identify the narrower class of organised research functions with a direct national security nexus.

The proposed reform would replace the current university-based and program-based model with a clearer statutory architecture. Capture would require an organised research function, a prescribed sensitive research field, a prescribed national security nexus pathway, and an identifiable responsible entity with governance, operational or management control of the function. This would make the framework more self-assessable and better targeted, while excluding ordinary teaching, individual researchers, isolated grants, one-off projects, incidental collaborations and ordinary commercial research activity that does not meet the prescribed criteria.

> Proposed model for consultation: Repeal the existing critical education asset class and replace it with a critical research asset class directed to a narrow class of nationally significant sensitive research functions. The asset class would not be limited to universities and could apply where equivalent research is conducted by another research entity.

The proposed model would require three cumulative elements:

- First, the research would need to be conducted through an organised research function for which an identifiable entity has governance, operational or management control. An organised research function could include a facility, platform, program, centre, laboratory, secure data environment or comparable arrangement operating on a sustained and centrally organised basis.
- Secondly, the research would need to fall within a sensitive research field prescribed in the Rules.
- Thirdly, the research would need to meet a prescribed national security nexus pathway.

No single factor would be sufficient on its own. Commonwealth funding, commercial value, dual-use potential or inclusion within a broad technology field would not, by itself, bring research within scope. Commonwealth funding would be relevant only where the Rules prescribe a particular Commonwealth, Defence or national capability program, contract, grant or arrangement as a national security nexus pathway.

Privately funded research could be captured only where it meets the same statutory architecture as other research. It would need to be conducted through an organised research function, fall within a prescribed sensitive research field, meet a prescribed national security nexus pathway, and have an identifiable responsible entity. Research would not be captured merely because it is commercially valuable, generally dual use, within a broad technology field, or because loss of intellectual property would affect an individual entity.

The Act would establish the asset class, the organised research function concept, the responsible entity, and the high-level criteria that constrain what fields and nexus pathways may be prescribed. The Definitions Rules would prescribe sensitive research fields, national security nexus pathways, thresholds and application settings following further consultation. Duplication with existing frameworks would be managed through the proposed exemptions framework where appropriate.

The Department's preliminary view is that Rules consultation should consider existing reference points such as the List of Critical Technologies in the National Interest, the Defence and Strategic Goods List, and AUKUS Pillar II Advanced Capabilities categories. Those references may help identify areas of potential sensitivity, but they were not designed as SOCI regulatory triggers. The prescribed fields and nexus pathways would therefore need to be tailored to SOCI's objectives, appropriately bounded, and subject to review and coordination across relevant agencies.

Key design elements

Element	Description
Cumulative capture model	A research function would only be captured where all required elements are met. The research would need to be conducted through an organised research function, fall within a sensitive research field prescribed in the Rules, meet a prescribed national security nexus pathway, and have an identifiable responsible entity. No single factor, including Commonwealth funding, commercial value, dual-use potential or inclusion within a broad technology field, would be sufficient on its own.

Element	Description
Prescribed sensitive research fields	The Rules would prescribe sensitive research fields that warrant SOCI capture. Research would not be captured merely because it is advanced, valuable or commercially significant. It would need to fall within a field prescribed because of its relevance to national security, the defence of Australia, or the security and resilience of one or more critical infrastructure sectors. Rules consultation would consider whether research domains outlined within existing references, such as the Defence and Strategic Goods List, AUKUS Pillar II categories, the List of Critical Technologies, or more tailored field descriptions, provide a stable and administrable basis for capture. The Rules may also need to account for fields where Australia has a concentrated or difficult-to-replace research strength and compromise, theft or misuse could have national consequences. The Rules may use one framework, a combination of frameworks or narrower descriptions where existing lists are too broad, too dynamic or insufficiently aligned with SOCI objectives.
Prescribed national security pathways	The national security nexus would be framed through prescribed pathways rather than an open-ended assessment of whether research is nationally significant. A research function would need more than inclusion within a prescribed sensitive research field. It would also need to meet a prescribed pathway that provides an objective connection to defence, intelligence, national security, export-controlled capability, classified or security-accredited environments, or another prescribed national capability of comparable sensitivity. Potential pathways could include research that: • is conducted under a contract, grant, arrangement or other instrument that includes prescribed defence, intelligence, national security, security-classified or protective security requirements • requires access to classified information, classified systems, security-accredited facilities or other protected Commonwealth systems or environments • involves technology, goods, software, source code, technical data or know-how subject to a prescribed export-control, sanctions, defence trade or comparable national security control framework • is conducted through a facility, platform, laboratory, secure data environment or comparable arrangement prescribed by class because of its security-sensitive function • is subject to prescribed Commonwealth security requirements, accreditation, sponsorship, clearance, access-control, or protective security conditions because of the sensitivity of the research, facility, data, technology or capability involved; or • meets a narrow reserve pathway where the Minister or Secretary determines that the organised research function has a direct and material connection to

Element	Description
	defence, national security or the security and resilience of one or more critical infrastructure sectors. Research would not meet the national security nexus merely because it is commercially valuable, dual-use in a general sense, Commonwealth funded, within a broad critical technology field, or indirectly relevant to a critical infrastructure sector.
Organised research function	Capture would attach to an organised research function, facility, platform, program, centre, secure data environment or comparable arrangement through which research is conducted on a sustained and centrally organised basis. The model is not intended to capture individual research activities, individual researchers, isolated grants or one-off projects. Whether a research activity is sufficiently sustained and centrally organised to constitute an organised research function would be determined by reference to factors prescribed in Rules or set out in guidance, and could include continuity of governance, continuity of infrastructure, and the existence of a defined research mission.
Responsible entity	The responsible entity would be the entity with primary governance, operational or management control of the organised research function. Practical control would be relevant where formal governance arrangements do not reflect the entity that can assess and manage the security risk in practice. Where research is conducted through a consortium, joint venture, collaborative centre, shared facility or secure data environment, the Act would establish a primary responsible entity test. The test would focus on which entity has primary responsibility for governing, operating or managing the organised research function, including control of the relevant facility or platform, control of access to sensitive information or technology, or responsibility for implementing security controls. The model would not make each participant, collaborator, funder or individual researcher a responsible entity merely because they contribute to, fund or participate in the research.
Coverage beyond universities	The framework would be capable of applying beyond universities where equivalent nationally significant research is conducted by public research bodies, private research entities, commercial entities, cooperative research structures, joint ventures or other collaborative arrangements. The model would focus on the research function and the entity best placed to manage the risk, rather than on whether the entity is a prescribed university.
Interaction with existing frameworks	Some research entities, facilities and programs may already be subject to security requirements through Defence contracts, the DISP, export controls, foreign interference settings, grant conditions, security accreditation, PSPF where relevant to Commonwealth entities, or other regulatory or contractual frameworks.

Element	Description
	The proposed exemptions framework, Rules design and guidance would be used to manage duplication where another framework delivers substantially equivalent or stronger outcomes. The intention is to avoid duplicative security requirements where existing arrangements already address the relevant risk, while preserving any SOCI obligations needed for residual visibility, assurance, notification or coordinated risk management.
What is not changing	The reform would not make the higher education and research sector a catch-all for research activity. Ordinary teaching, ordinary commercial research and development, isolated grants, one-off projects, individual research activities, individual researchers and incidental collaborations would remain outside scope unless they form part of an organised research function that meets the prescribed field, prescribed national security nexus pathway and responsible entity requirements.

Preliminary Impact Analysis

This measure would reset the regulatory perimeter for critical research assets. Some universities that are currently captured because they own or operate an asset used for a program of research may fall outside scope if the relevant research does not meet the proposed cumulative model. Some non-university research entities may come into scope where they have governance, operational or management control of an organised research function that falls within a prescribed sensitive research field and meets a prescribed national security nexus pathway. The final affected population would depend substantially on Rules-level settings, including the sensitive research fields, national security nexus pathways, thresholds, exclusions, reserve pathway and treatment of collaborative research structures.

The expected costs for newly captured entities would comprise both one-off transition costs and ongoing compliance costs. One-off costs would arise from assessing whether research functions meet the revised criteria, identifying the responsible entity for collaborative facilities, platforms, centres, laboratories or secure data environments, registering captured assets, and establishing or extending risk management arrangements (where applicable). Ongoing costs would arise from maintaining those arrangements, annual reporting, incident reporting and any coordination needed across consortium, joint venture or shared-facility models. For research functions already subject to comparable legal or administrative frameworks, or contractual requirements, the incremental cost may be lower where equivalent arrangements can be recognised through Rules settings, guidance or the proposed exemptions framework.

The measure is expected to have a limited effect on competition, innovation or market entry as the intent is for the Rules to be calibrated to capture only nationally significant sensitive research functions with a direct national security nexus. Ordinary teaching, individual researchers, isolated grants, one-off projects, incidental collaborations and ordinary commercial research activity would remain outside scope unless the cumulative statutory requirements are met.

Consultation questions

66. Is the proposed three-part model a clear and workable basis for identifying nationally significant sensitive research functions? Are an organised research function, a prescribed sensitive research field and a prescribed national security nexus pathway the right cumulative elements?

67. What should be used to prescribe sensitive research fields and national security nexus pathways in a way that is objective, administrable and appropriately bounded? How should the framework use references such as the Defence and Strategic Goods List, AUKUS Pillar II categories, the List of Critical Technologies, export-control settings, classified-access settings, security-accredited facilities or more tailored field descriptions without making those references self-executing SOCI triggers?

68. Does the proposed organised research function model provide a workable way to identify the regulated function while excluding individual researchers, individual research activities, isolated grants, one-off projects and incidental collaborations?

69. In collaborative structures, shared facilities, secure data environments, centres, consortia or joint ventures, what factors should identify the primary responsible entity with governance, operational or management control of the organised research function?

70. Should privately funded research be capable of capture where it meets the same statutory architecture as other research? Should there be a separate pathway for exceptional concentrated or difficult-to-replace Australian research capability, and what safeguards should apply?

71. How should SOCI interact with existing Defence, export-control, foreign interference, grant, accreditation, PSPF or contractual security requirements so that equivalent arrangements are recognised and unnecessary duplication is avoided?

Part C – Governance, Assurance and Accountability

Measure 15 – CIRMP Governance and Assurance

This measure addresses how responsible entities govern, review and assure their Critical Infrastructure Risk Management Programs (CIRMPs). The current regime relies heavily on self-attestation and contains review and currency obligations that can be difficult to apply consistently. This can make it harder for entities, governing bodies and regulators to know whether a CIRMP is current, implemented and working in practice

The proposed reforms have three linked parts: removing current limits on the use of annual compliance reports in civil penalty proceedings, strengthening CIRMP governance and review obligations, and introducing proportionate assurance of CIRMP design, implementation and effectiveness

Improving harmonisation with the *Foreign Acquisitions and Takeovers Act 1975*: The Department recognises that some foreign-owned entities may already be subject to reporting, audit or assurance conditions under the foreign investment framework. The Department would engage with Treasury during implementation to identify opportunities to reduce duplication. This may include considering whether SOCI reporting or assurance outcomes could support variation or sunsetting of overlapping FATA conditions where those conditions address equivalent risk-management, reporting or assurance outcomes.

A. Removing admissibility restrictions

The problem

The current admissibility restrictions prevent the CISC from relying on mandatory annual compliance reports as evidence in civil penalty proceedings, even where those reports disclose potential non-compliance. This creates a disconnect between the framework's primary compliance-reporting mechanism and its enforcement architecture.

Annual compliance reports are mandatory statutory compliance and assurance documents. They are intended to provide evidence of whether the entity is complying with its CIRMP obligations. Where a report is materially false, misleading, incomplete, or relevant to serious or repeated non-compliance, the report itself may be directly relevant to the integrity of the entity's compliance posture.

The current restriction can also make the reporting framework less efficient. If an annual report discloses non-compliance, the regulator may need to obtain the same underlying evidence through compulsory information-gathering powers. This can add process without improving certainty for entities or changing whether enforcement action is available in appropriate cases.

Proposed model for consultation: Repeal the current admissibility restrictions in sections 30AG and 30AQ so that annual compliance reports may be relied on in civil penalty proceedings where appropriate.

The policy intent is to make annual compliance reports part of the ordinary reporting, assurance and enforcement framework The reform would not require enforcement action because an entity has

disclosed non-compliance. Voluntary disclosure, cooperation and timely remediation would remain relevant to compliance and enforcement decision-making.

Mandatory annual compliance reports should be capable of being used where they are relevant to serious or repeated non-compliance, or where a report is materially false, misleading or incomplete. The Department is seeking views on whether any safeguards or limits should apply to the use of annual compliance reports in civil penalty proceedings.

B. Strengthened governance controls

The problem

The current CIRMP framework does not provide sufficiently clear governance, review and currency obligations. The Act requires CIRMPs to be reviewed "regularly" and kept "up to date", but those standards are not defined with enough precision to support consistent supervision or provide industry with clear expectations. There is also no clear statutory requirement for the governing body or a sufficiently senior decision-maker to approve the establishment, review, update and variation of the CIRMP itself.

This matters because decisions about risk appetite, security investment, prioritisation and remediation are usually made at board or senior-management level. If CIRMP governance is not clearly connected to those decision-makers, the program can become a compliance document rather than a practical tool for managing risk, setting priorities and funding remediation.

Proposed model for consultation: Strengthen CIRMP governance by requiring the governing body, or in specified circumstances a nominated senior manager, to approve the establishment, review, update and variation of the CIRMP and to exercise ongoing oversight of risk identification and management under it.

The Act would also prescribe a minimum review cycle and clearer event-based triggers for earlier review. The proposed starting point is that a CIRMP should be reviewed at least once every 24 months, and earlier where specified events occur. Those events could include a significant cyber security incident affecting the asset, a material change to the asset's operating environment, ownership structure or supply chain, relevant risk information communicated by the Department, or a relevant finding from an audit, assurance activity, cyber security exercise or vulnerability assessment.

The Act would also set clearer criteria for when a CIRMP is not up to date. Those criteria could include whether the CIRMP reflects the entity's current operating environment and asset configuration, current threats and hazards, current regulatory requirements, current governance arrangements, and lessons learned from relevant incidents, exercises or reviews.

The policy intent is to make CIRMP governance easier to understand and demonstrate. Responsible entities would have clearer expectations about who must approve the CIRMP, when it must be reviewed, and what it means for the CIRMP to remain current.

C. Independent CIRMP assurance

The problem

The current regime relies heavily on self-assessment and governing-body attestation as the primary mechanisms for assuring CIRMP compliance. Annual reporting provides an important compliance signal, and governing-body approval supports senior accountability. However, these mechanisms provide limited

independent evidence that the CIRMP is adequate, implemented in practice, operating effectively, or accurately reflected in the entity's annual report.

This creates practical uncertainty for responsible entities, governing bodies and regulators. A board may approve an annual report without having a consistent independent basis for understanding whether the CIRMP reflects the entity's actual operating environment, whether key controls are working, whether material dependencies are being managed, or whether remediation activity is addressing the right issues. Responsible entities may also receive limited external feedback until a regulator-led audit, incident, exercise or compliance engagement identifies a problem.

The current settings can therefore make it harder to identify gaps early, prioritise remediation, and show that the CIRMP is more than a static compliance document. They can also leave governing bodies without enough evidence to oversee security resourcing, risk appetite, dependency management and remediation decisions.

The CISC audit program provides some independent verification, although regulator-led audits cannot provide broad assurance coverage across the regulated population in each reporting cycle. Periodic independent assurance would provide a more scalable way to test whether CIRMPs are current, implemented and effective in practice.

Any assurance model would need to be proportionate. A large, complex or highly critical asset may warrant a different level of assurance from a smaller or lower-risk asset. Without proportionality, assurance could impose unnecessary cost without improving security outcomes.

The policy problem is that the current framework does not provide a consistent, scalable and proportionate assurance baseline across responsible entities.

Proposed model for consultation: Require responsible entities to obtain periodic independent assurance of the design, implementation, appropriateness and operational effectiveness of their CIRMP.

The assurance process would assess whether the CIRMP is implemented and operating effectively, remains appropriate having regard to the entity's current operations, asset profile and risk environment, is aligned to the entity's governance settings, risk tolerances and criticality profile, and is supported by adequate resources, capability, systems and oversight.

The base review cycle would be at least once every three years. The scope, method, frequency and independence requirements would be calibrated to the nature, size, complexity and criticality of the responsible entity and the relevant asset, the entity's operating profile and dependency landscape, and the risks arising from applicable hazard vectors.

For lower-risk entities, an internal assurance function may be sufficient where it is operationally independent from the design and operation of the CIRMP and has appropriate capability. More frequent review, or stronger independence requirements, could apply where warranted by the entity's risk profile, including for assets of heightened national, economic or societal importance, where the threat environment is elevated, or where there have been significant changes to the asset, operating environment or risk posture.

Assurance reports would be provided to the entity's governing body and to the CISC. Where material deficiencies are identified, the responsible entity would be required to prepare and provide a remediation plan. Where a review identifies a serious deficiency within the meaning of section 30AI, the

report may provide an evidential basis for the CISC to consider use of its existing CIRMP remediation powers.

Key design elements: independent CIRMP assurance

Element	Description
Scope of review	The review would assess whether the CIRMP is appropriately designed, implemented and operating effectively. It would also assess whether the CIRMP remains appropriate to the entity's current operations, asset profile, dependencies and risk environment; aligns with the entity's governance settings, risk tolerances and criticality profile; is supported by adequate resources, capability, systems and oversight; and is accurately reflected in the written program and supporting records.
Proportionality	Review frequency, scope, method and independence requirements would be proportionate to the responsible entity and the asset. Relevant factors would include the asset's criticality, the entity's size and complexity, its operating profile and dependencies, and the risks arising from applicable hazards. The base cycle would be at least once every three years. More frequent review, or stronger independence requirements, could apply where the asset is of heightened national, economic or societal importance, where the threat environment is elevated, or where there have been significant changes to the asset, operating environment, dependencies or risk posture.
Independence	The reviewer would need to be operationally independent from the design, implementation and operation of the CIRMP, and appropriately trained, competent and experienced having regard to the nature of the asset and the hazard vectors being assessed. Independence requirements would be proportionate to the nature, size, complexity and criticality of the responsible entity and the relevant asset. Where warranted by risk profile, independence requirements may include restrictions on the reviewer having provided consulting or advisory services relating to the development or implementation of the CIRMP within a specified look-back period, limitations on material financial or commercial relationships beyond the assurance engagement, and disclosure of actual or potential conflicts of interest to the responsible entity and the CISC. For lower-risk entities, an internal assurance function may be sufficient where it is demonstrably independent from the design and operation of the CIRMP and has appropriate capability.
Reporting and remediation	The reviewer would provide a written report to the responsible entity's board, board risk committee or other governing body responsible for CIRMP oversight, and to the CISC. The report would be provided within a specified period after the review is completed. Where the review identifies material deficiencies, the responsible entity would be required to prepare and provide a remediation plan addressing those deficiencies

Element	Description
	within a specified period. Where the review identifies a serious deficiency within the meaning of section 30AI, the report may provide an evidential basis for the CISC to consider use of its existing CIRMP remediation powers.
Cost	The responsible entity would bear the cost of the review, in line with comparable regulatory regimes. The proportionality settings for scope, frequency and independence are intended to ensure that the cost of assurance is commensurate with the nature, size, complexity and criticality of the entity and asset.
Assurance standards and guidance	Detailed expectations for assurance scope, reviewer capability, independence, conflicts of interest, reporting format and examples of acceptable assurance models would be developed through Rules or guidance. This would support consistency across assurance providers while allowing the model to be calibrated for different sectors, asset classes and risk profiles.
Material changes outside the ordinary cycle	Outside the ordinary assurance cycle, a responsible entity would assess whether its CIRMP remains appropriate if there is a material change to the asset's nature, size, complexity, operating environment, dependencies or risk posture. If the assessment shows that the CIRMP needs to change, the entity would update it as soon as practicable. The independent assurance framework would complement, rather than replace, the entity's ongoing governance, review and currency obligations.

Preliminary Impact Analysis

This measure is likely to increase regulatory costs for responsible entities subject to CIRMP obligations. The increase would be greatest for entities that do not already undertake independent assurance of their security risk management arrangements or maintain mature board-level review processes. Entities with established governance and assurance arrangements would face a smaller uplift, so the impact would be uneven across the regulated base.

The main costs comprise strengthened governance and approval processes, periodic independent assurance, preparation and review of assurance reports, remediation where deficiencies are identified, and engagement with the CISC on assurance outcomes. These costs would vary with the size, complexity and criticality of the entity and asset, the maturity of existing assurance arrangements, and the extent to which internal or equivalent external assurance can be recognised. The recurring cost of periodic independent assurance is expected to be the most material ongoing element of this measure.

The measure may reduce duplication where SOCI assurance can be aligned with existing audit, prudential or assurance requirements. The effect on competition and market entry is expected to be limited, although costs may be more significant for entities with limited access to suitably qualified assurance providers, including smaller responsible entities and regional operators. For those entities, assurance may be harder to source and proportionally more expensive.

Consultation questions

72. Should the current admissibility restrictions on annual compliance reports be removed entirely, or should any limitations on use be retained? If safeguards are needed, what should they be?

73. Is a clearer governance and review framework, including governing-body or senior-manager approval, a minimum review cycle and event-based triggers for earlier review, the right way to improve CIRMP currency and accountability?

74. Are the proposed CIRMP currency criteria appropriate, including whether the CIRMP reflects the entity's current operating environment and asset configuration, current threats and hazards, current regulatory requirements, current governance arrangements, and lessons learned from incidents, exercises or reviews?

75. Should periodic independent assurance be mandatory for responsible entities subject to CIRMP obligations? If so, is a three-year base cycle appropriate?

76. What assurance models should be acceptable for different risk profiles, including external assurance, internal audit or other operationally independent assurance functions?

77. In what circumstances should more frequent review or stronger independence requirements apply?

78. Should assurance reports be provided to both the responsible entity's governing body and the CISC? What timeframes should apply for reports and remediation plans where material deficiencies are identified?

Measure 16 – Graduated Civil Penalty Settings

The problem

The SOCI Act already uses a graduated civil penalty structure. Lower-tier administrative and visibility obligations generally attract lower maximum penalties. Core preventive and assurance duties, including many obligations relating to critical infrastructure risk management programs, incident response planning, cyber security exercises and vulnerability assessments, are generally set at 200 penalty units.

At the upper end of the scheme, more security-critical obligations already attract materially higher penalties. This includes 1,500 penalty units for the obligation to protect critical telecommunications assets and 2,000 penalty units for non-compliance with a Ministerial direction under Part 2D. Separate consultation is also being undertaken on proposed penalty settings for non-compliance with Ministerial directions under Part 3.

This structure reflects an existing distinction in the Act between administrative requirements, preventive and assurance duties, and the most serious intervention-related obligations. Practical experience with the framework suggests that the current 200 penalty unit setting may no longer reflect the significance of selected preventive and assurance duties.

Those duties are central to the operation of the SOCI framework. Obligations to establish, maintain, comply with, review and update risk management and assurance mechanisms are the means by which responsible entities identify material risks, implement controls, test preparedness and remediate deficiencies.

Non-compliance with those duties can leave material risks unidentified, untreated or untested, and can reduce an entity's ability to sustain, restore or resume essential services during or after a serious incident.

The Independent Review identified broader concerns that the SOCI framework is perceived as too focused on administration and documentation, and insufficiently focused on effective risk management, testing, remediation and accountability. This points to a gap in the current penalty settings. Selected preventive and assurance duties sit above routine administrative obligations, but their current maximum penalty may not provide a strong enough accountability signal for duties that are central to risk management, preparedness and remediation.

The policy problem is therefore confined to the middle tier of the existing penalty structure. It does not concern lower-tier administrative and visibility obligations, or the highest penalties for serious telecommunications and direction-related obligations.

Proposed model for consultation: Increase the maximum civil penalty for selected core preventive and assurance duties from 200 penalty units to 500 penalty units.

The proposed uplift would apply to obligations that sit at the centre of the Act's preventive and assurance architecture. This includes obligations to have, comply with, review and update critical infrastructure risk management programs and equivalent assurance settings, together with related obligations concerning incident response planning, cyber security exercises, vulnerability assessments and associated compliance architecture.

The uplift would strengthen deterrence for non-compliance with duties that support risk identification, preparedness, assurance, testing and remediation. It would preserve a clear distinction between the middle tier and the higher penalties already reserved for the most serious telecommunications and direction-related obligations.

Lower-tier administrative and visibility obligations, including routine reporting, entity-change notifications and cyber incident notification requirements, would remain at their existing settings. Separate reforms relating to penalties for non-compliance with Ministerial directions under Part 3 are being consulted on through the Tranche 1 directions process.

The proposed uplift would operate within the existing enforcement framework in Part 5 of the SOCI Act and the *Regulatory Powers (Standard Provisions) Act 2014*. The court would continue to determine the appropriate pecuniary penalty in the circumstances of the case, up to the statutory maximum. The court would continue to take into account all relevant matters, including the nature and extent of the contravention, loss or damage, the circumstances in which the contravention took place, and any previous similar contraventions.

A 500 penalty unit maximum would recalibrate the middle tier without changing the Act's graduated structure. It would sit above the current 200 penalty unit settings for many core preventive and assurance duties, and well below the 1,500 to 2,000 penalty unit settings used for the Act's most serious obligations.

Key design elements

Element	Description
Targeted middle-tier uplift	The measure would apply only to selected core preventive and assurance duties that support risk identification, preparedness, testing, assurance and remediation. Other civil penalty provisions would remain at their current settings.
500 penalty unit maximum	The proposed new maximum for selected provisions would be 500 penalty units. This would recalibrate the middle tier while preserving court discretion to impose a lower penalty where appropriate in the circumstances of the case.
Lower-tier obligations unchanged	Lower-tier administrative and visibility obligations, including routine reporting, entity-change notifications and cyber incident notification requirements, would remain at their existing settings.
Top-tier obligations unchanged	Existing or separately proposed higher penalties for security-critical telecommunications obligations and non-compliance with Ministerial directions would remain separate from this measure.
Existing enforcement framework preserved	Civil penalty orders, injunctions, enforceable undertakings, monitoring, investigation and court-based penalty determination would continue under the existing enforcement framework.
Court discretion and proportionality	The proposed penalty would be a statutory maximum, not an automatic penalty. The court would continue to determine the appropriate penalty in each case by reference to the circumstances of the contravention, including seriousness, harm, culpability, cooperation, remediation and any history of similar conduct.

Preliminary Impact Analysis

This measure would recalibrate the maximum civil penalty for selected preventive and assurance duties. It would not introduce any new compliance activity, so no entity would acquire a new obligation, and the underlying obligations would remain unchanged.

The associated costs are expected to be one-off. They would comprise familiarisation with the revised settings, legal or compliance review of the affected obligations, and any voluntary compliance uplift undertaken by entities that identify gaps when reassessing their exposure. The measure is not expected to adversely affect competition, innovation or market entry. It would preserve the graduated structure of the SOCI Act by retaining lower-tier administrative duties at existing settings and reserving higher penalties for the most serious telecommunications and direction-related obligations.

Consultation questions

79. Are the selected preventive and assurance duties the right obligations for the proposed 500 penalty unit maximum? Are there any obligations that should be added or excluded?

80. Does a 500 penalty unit maximum provide a proportionate middle-tier setting between lower-tier administrative obligations and higher-tier telecommunications or Ministerial direction obligations?

81. Would the proposed uplift create any material compliance review costs for responsible entities? If so, what activities or costs would be involved?

Measure 17 – Operations and Maintenance and Managed Service Providers

The problem

The SOCI Act generally places obligations on the entity that owns, operates or has legal responsibility for a critical infrastructure asset. That remains the right starting point. In practice, however, key operational functions are increasingly performed by third parties, including outsourced operators, managed service providers, original equipment manufacturers (OEMs), platform administrators and other contractors. These entities may not own the asset, hold a direct interest in it, or otherwise fall within the current framework.

This creates a practical gap where an entity outside the existing framework exercises material operational control over the asset, or over a critical function, system or service on which the asset materially depends. That entity may control access pathways, operational settings, dispatch outcomes, configuration, remote maintenance, restoration processes or specialist technical systems. Its systems, decisions or failures may directly affect the operation, availability, integrity or security of the asset.

The responsible entity should remain the primary regulated entity. It remains best placed to hold the broader SOCI obligations for the asset, including the obligation to establish and maintain a CIRMP. The current framework, however, does not deal consistently with third parties that exercise practical operational control over critical functions without holding ownership or direct-interest positions.

This can create uncertainty for responsible entities about how to manage those operational dependencies through their CIRMP, incident response, assurance and remediation arrangements. It can also slow regulatory engagement where the person best placed to provide information or take action is the third-party operator, platform administrator, OEM or managed service provider.

The policy problem is that the current framework may not give Government or responsible entities sufficient visibility of third parties with practical control over critical functions, or provide a clear basis for those third parties to cooperate, notify relevant changes, or avoid actions that could materially compromise the asset.

Proposed model for consultation: Introduce a new concept of a "relevant operator" to identify entities that exercise material practical control over a critical infrastructure asset, or over a critical function, system or service on which the asset materially depends, without being the responsible entity.

A person would be a relevant operator only where both practical operational authority and material operational dependency are present. Practical operational authority may include the ability to operate, configure, maintain, disable, restore, materially alter or materially influence the operation, availability, integrity or security of the asset or critical function. Material operational dependency would arise where

the responsible entity depends on the exercise of that control for the continued operation, availability, integrity or security of the asset.

The reform would have three linked elements:

- First, relevant operators would be identified and made visible to Government through calibrated registration and information obligations. The responsible entity would provide information about relevant operators and the nature of the arrangement. The relevant operator would provide information within its own knowledge and control.
- Secondly, the reform would clarify that the responsible entity remains responsible for compliance with its CIRMP obligations and must maintain appropriate arrangements with relevant operators where it depends on them for critical functions. Those arrangements may support compliance, incident response, access to information, oversight, assurance, testing and remediation.
- Thirdly, relevant operators would be subject to limited direct duties proportionate to their role. These would include a duty to cooperate with the responsible entity's compliance with Part 2A, a duty to notify the responsible entity of events, changes or circumstances within the operator's knowledge that could materially affect the asset, and a duty not to take or omit to take action that the operator knows or ought reasonably to know would materially compromise the security, integrity, availability or operation of the asset.

The responsible entity would remain the primary regulated entity and would not be relieved of its broader SOCI obligations. The relevant operator would not become subject to the full responsible-entity obligation set merely because it is identified or registered. Its direct duties would be limited to matters within its own role, knowledge and practical control.

The direct duties imposed on a relevant operator would be statutory duties enforceable against that operator. The relevant operator would be liable only for contraventions of duties imposed directly on it, and not for the responsible entity's broader SOCI obligations.

The framework could apply in layered contractual and outsourced operating models, including to subcontractors or downstream service providers, but only where they themselves exercise material practical control over the asset or critical function. Subcontractor status alone would not be enough.

The framework would include a limited safe harbour for responsible entities that take reasonable steps to secure appropriate arrangements with a relevant operator and cannot do so. The safe harbour would apply only to the duty to maintain those arrangements and would require a written request, evidence of refusal or inadequate response, a documented mitigation plan, and disclosure through annual reporting.

Key design elements

Element	Description
Relevant operator concept	The framework would identify entities that exercise material practical control over a critical infrastructure asset, or over a critical function, system or service on which the asset materially depends. The concept would turn on two elements: practical operational authority and material operational dependency. Practical operational authority may include the

Element	Description
	ability to operate, configure, maintain, disable, restore, materially alter or materially influence the operation, availability, integrity or security of the asset or critical function. Material operational dependency would arise where the responsible entity depends on the exercise of that control for the continued operation, availability, integrity or security of the asset. The concept would be assessed by what the entity can do in practice, not by its contractual label. It would not depend on whether the entity is described as an operator, managed service provider, maintenance provider, OEM, platform provider or contractor.
Exclusions and boundaries	The mere provision of professional advice, monitoring-only services, minor maintenance, emergency support, commodity inputs, general-purpose infrastructure, software support, equipment supply or ordinary subcontracted services would not be sufficient. Capture would require substantive practical control over the asset or critical function, or express capture under another SOCI provision. Monitoring without authority to act, maintenance that cannot materially affect operation, availability or security without further instruction, and emergency step-in exercised at the responsible entity's direction for a limited period would generally remain outside scope. General-purpose infrastructure services, including cloud computing, telecommunications carriage and electricity supply, would remain outside scope unless the provider exercises direct operational control over a critical function of the specific asset.
Targeted registration and information	Relevant operators would be identified through calibrated registration and information obligations. The responsible entity would identify relevant operators and provide prescribed information about the arrangement. The relevant operator would provide prescribed information within its own knowledge and control. Information could include the relevant operator's identity and contact details, the functions, systems or components the relevant operator controls or operates, the nature and duration of the arrangement, and any other information prescribed by the Rules. A relevant operator's registration obligation would be limited to operations and maintenance information for this measure. Registration would not make the relevant operator a responsible entity and would not make it subject to the full suite of Part 2 reporting obligations.
Responsible entity remains primary	The responsible entity would remain the primary bearer of CIRMP and other core obligations. The responsible entity's Part 2A obligations would remain non-delegable. Where the responsible entity depends on a relevant operator for critical functions, it would be required to maintain appropriate contractual, governance

Element	Description
	or operational arrangements to support compliance, incident response, access to information, oversight, assurance, testing and remediation.
Operational dependency management	Where a responsible entity relies on one or more relevant operators, its CIRMP would need to address the risks created by that dependency. This may include risks relating to the relevant operator's access to systems and data, the effect on continuity if the operator fails, withdraws or is compromised, and the responsible entity's ability to oversee, audit and remediate the operator's performance.
Limited direct obligations on the relevant operator	Relevant operators would be subject to a limited set of direct obligations proportionate to their role and control. The framework is intended to include: • a duty to cooperate, so far as reasonably practicable, with the responsible entity's compliance with Part 2A, including by providing reasonable access to information, systems and personnel where needed for risk management, assurance, incident response or remediation • a duty to notify the responsible entity, without unreasonable delay, of events, changes or circumstances within the operator's knowledge that could materially affect the operation, availability, integrity or security of the asset • a duty not to take, or omit to take, action that the operator knows or ought reasonably to know would materially compromise the security, integrity, availability or operation of the asset, except where acting under a lawful direction, court order or statutory requirement. The duties would apply only to matters within the relevant operator's role, knowledge and practical control.
Duty not to materially compromise	The duty not to materially compromise the asset would apply to conduct or omissions within the relevant operator's role and practical control. It could include misuse of legitimate access, unsafe or unauthorised configuration changes, manipulation of control systems, pre-positioning for later compromise, or unauthorised exposure or redirection of security-relevant data flows. The duty would be directed to material compromise of the security, integrity, availability or operation of the asset or critical function. It would not apply to matters outside the relevant operator's knowledge, role or practical control.
Protected information	The framework would support appropriate sharing of protected information between responsible entities and relevant operators where necessary for compliance, incident response, assurance, remediation or directions. Relevant operators that receive or hold protected information would be subject to the applicable protected information obligations.
Enforcement against relevant operators	Relevant operators would be brought within the SOCI enforcement framework for the direct duties imposed on them. The cooperation duty, notification duty

Element	Description
	and duty not to materially compromise the asset would be civil penalty provisions enforceable against the relevant operator. The existing enforcement tools in Part 5 of the SOCI Act would apply to those duties. This would allow civil penalty proceedings and other available enforcement responses to be taken directly against the relevant operator where it contravenes a duty imposed on it. A relevant operator would be liable only for its own statutory duties. Registration as a relevant operator would not make the operator responsible for the responsible entity's broader SOCI obligations. Where a Ministerial direction relates to a critical infrastructure asset and compliance requires action within a relevant operator's direct control, the framework could allow the direction to be given to the relevant operator for those matters. This would ensure that a direction can be addressed to the entity capable of taking the required operational action.
Safe harbour for responsible entities	Where a responsible entity cannot secure arrangements with a relevant operator that are reasonably necessary to support compliance with Part 2A, a limited safe harbour is under consideration. To rely on the safe harbour, the responsible entity would need to have made a written request seeking the necessary arrangements. The relevant operator must have refused, failed to respond within a reasonable period or agreed only to inadequate terms. The responsible entity would also need to implement a documented mitigation plan for the residual risk and record its reliance on the safe harbour through the annual reporting framework. The safe harbour would be limited to the duty to maintain arrangements with the relevant operator. It would not relieve the responsible entity of its broader obligations under the Act.
What is not changing	The reform would preserve the responsible entity model. The responsible entity would remain the primary regulated entity for the asset and would continue to bear the broader SOCI obligation set. The reform would create targeted visibility and limited direct duties for third parties that exercise material practical control over the asset or a critical function. Outsourced providers, suppliers, OEMs, subcontractors, software vendors and platform providers would remain outside scope unless they meet the relevant operator test or another defined statutory pathway.

Preliminary Impact Analysis

This measure is likely to bring some operations and maintenance providers, managed service providers, OEMs, platform administrators and other outsourced operators within SOCI where they exercise material practical control over a critical infrastructure asset or critical function. The affected population would be defined by practical control, not by sector. Providers operating across several critical infrastructure sectors are therefore the most likely to be captured.

The main costs arise from assessing whether an entity is a relevant operator, registering relevant operator information, updating contracts and operational protocols, and complying with limited direct duties to cooperate, notify and avoid materially compromising the asset. Responsible entities may also incur costs in mapping operational dependencies and updating CIRMP arrangements to reflect reliance on relevant operators. The most widespread cost is expected to be the updating of contracts, because it affects existing service agreements.

The measure is expected to affect mainly medium and large providers. The effect on competition and market entry is expected to be limited if the relevant operator concept is confined to entities with material practical control. A broader concept could affect smaller providers, offshore support models and subcontractors, and may have a greater effect in sectors where managed services are concentrated among a small number of providers.

Consultation questions

82. Does the proposed "relevant operator" concept identify the right class of entities? Should the test require both practical operational authority and material operational dependency?

83. Are the proposed exclusions and boundaries sufficiently clear for advisory services, monitoring-only arrangements, minor maintenance, emergency support, general-purpose infrastructure, software support, equipment supply and ordinary subcontracting?

84. Are the proposed direct obligations on relevant operators proportionate to their role and control, including duties to cooperate, notify and avoid materially compromising the asset? What enforcement tools and penalty settings should apply to those duties?

85. Is the proposed safe harbour for responsible entities workable where they cannot secure appropriate arrangements with a relevant operator? What evidence, mitigation and reporting requirements should apply?

86. What practical issues arise for foreign operators, subcontractors or entities with limited Australian presence, including where direct engagement or directions may be needed for matters within the operator's control?

Measure 18 – Corporate Group Cooperation

The problem

The current SOCI framework places obligations on a single responsible entity for each critical infrastructure asset. In practice, critical infrastructure is often held within a corporate group in which functions material to the security of the asset are controlled by a parent company, shared services entity or another related body corporate. Those functions may include cyber security, workforce management, procurement, shared IT, governance, physical security, supply chain management or operational decision-making.

This can create practical difficulty for the responsible entity. The responsible entity may be required to establish, maintain, comply with and review a CIRMP, while the information, systems, people, contracts, security controls or decision-making authority needed to do so sit elsewhere in the corporate group.

The current framework does not provide a direct cooperation mechanism for those circumstances. A connected entity that controls a function material to CIRMP compliance may have no statutory duty to assist the responsible entity, provide relevant information, avoid frustrating compliance, or notify incidents, changes or circumstances that affect the responsible entity's ability to manage risks to the asset.

The policy problem is that a responsible entity may be legally accountable for CIRMP compliance, while another entity in the same corporate group controls the information, systems, people or decisions needed for that compliance. This can make risk management harder, slow incident response, and leave important dependencies unmanaged or unclear.

Proposed model for consultation: Where a responsible entity has a material CIRMP dependency on a connected entity within its corporate group, impose a limited statutory duty on that connected entity to cooperate.

A material CIRMP dependency would exist where the responsible entity relies on the connected entity to provide, manage or control a function that is material to the responsible entity's ability to comply with its CIRMP obligations. This may include functions relevant to cyber and information security, personnel security, supply chain security or physical security.

The duty would require the connected entity, to the extent reasonable in the circumstances, to support the responsible entity's CIRMP compliance. It would include three limbs:

- a duty not to take action, or fail to take action, that the connected entity knows or ought reasonably to know would materially prevent or undermine the responsible entity's CIRMP compliance
- a duty, on reasonable request, to provide information, access or assistance reasonably necessary for the responsible entity to establish, maintain, comply with and review its CIRMP
- a duty to notify the responsible entity of incidents, changes or circumstances that could materially affect the security of the asset or the responsible entity's ability to manage CIRMP risks.

The connected entity would not become the responsible entity for the asset and would not assume the responsible entity's full CIRMP obligations. The responsible entity would remain primarily responsible for adopting, maintaining, reviewing and complying with the CIRMP.

The cooperation duty would arise where the material CIRMP dependency exists. Visibility of those dependencies would be supported through the broader Register reform package, particularly the proposed systems, suppliers and dependencies information category. Registration or disclosure would support evidence of the dependency, although the duty itself would not depend on prior registration.

The framework would be designed to operate across complex corporate group structures, including offshore holding structures, trusts, joint ventures, layered holding companies, shared services entities and special purpose vehicles. The reasonableness qualifier would keep the duty proportionate by taking account of the nature of the dependency, the connected entity's role and capability, the burden of assistance, and any legal or regulatory constraints affecting cooperation.

Key design elements

Element	Description
Connected entity	The concept would cover related bodies corporate and other entities within the same corporate group where they are under common control with the responsible entity. This may include parent companies, subsidiaries, shared services entities and other group entities, including foreign-incorporated entities where relevant. The framework would need to operate across complex corporate structures, including offshore holding structures, trusts, joint ventures, layered holding companies, shared services entities and special purpose vehicles. The duty would arise only where the responsible entity has a material CIRMP dependency on the connected entity.
Material CIRMP dependency	The duty would arise where the responsible entity relies on the connected entity to provide, manage or control a function that is material to the responsible entity's ability to comply with its CIRMP obligations. This may include functions relevant to cyber and information security, personnel security, supply chain security or physical security. Examples could include group-wide IT systems, security operations centres, identity and access management, workforce screening, procurement, vendor management, shared physical security functions, governance approvals or incident response capability.
Cooperation duty	The connected entity would be required, to the extent reasonable in the circumstances, to cooperate with the responsible entity's CIRMP compliance. The duty would include three limbs: • the connected entity must not take action, or fail to take action, that it knows or ought reasonably to know would materially prevent or undermine the responsible entity's ability to comply with its CIRMP obligations • on reasonable request, the connected entity must provide information, access or assistance reasonably necessary for the responsible entity to establish, maintain, comply with and review its CIRMP; and • the connected entity must notify the responsible entity of incidents, changes or circumstances that could materially affect the security of the asset or the responsible entity's ability to manage CIRMP risks.
Enforcement of the connected entity duty	The connected entity would not become the responsible entity for the asset and would not assume the responsible entity's full CIRMP obligations. The responsible entity would remain primarily responsible for adopting, maintaining, reviewing and complying with the CIRMP. The connected entity would be liable only for breach of its own limited cooperation duty. This could include unreasonably failing to provide information or assistance needed for the responsible entity's CIRMP compliance, frustrating the responsible entity's compliance, or failing to

Element	Description
	notify incidents, changes or circumstances that materially affect the responsible entity's ability to manage risks to the asset. Breach of the cooperation duty would attract a civil penalty. A 200 penalty unit maximum is being considered, consistent with the existing penalty framework for core Part 2A obligations and reflecting the supporting nature of the connected entity duty. The existing compliance and enforcement framework, including infringement notices, enforceable undertakings, injunctions and civil penalty proceedings, could apply to breach of the connected entity duty.
Proportionate operation	The duty would be subject to a reasonableness qualifier, so it operates proportionately to the nature of the dependency and the size, capability and role of the connected entity. Relevant factors may include the seriousness and urgency of the risk, the connected entity's access to relevant information or systems, the extent of its control over the relevant function, the burden of providing assistance, confidentiality obligations, foreign law constraints, regulatory restrictions and any other legal constraints affecting cooperation.
Interaction with Register reform	Visibility of material dependencies would be supported through the broader Register reform package, particularly the proposed systems, suppliers and dependencies information category. The Register could require responsible entities to identify material dependencies on related bodies corporate or other entities within the same corporate group and describe the nature of the dependency. The cooperation duty itself would arise where the material CIRMP dependency exists. Prior registration would not be a precondition for the duty to arise.
Foreign connected entities	The framework would be capable of applying to foreign-incorporated connected entities where they are within the same corporate group and the responsible entity has a material CIRMP dependency on them. Practical enforcement may depend on the connected entity's Australian presence, assets, conduct or other jurisdictional connection. The reasonableness qualifier would also account for foreign law, regulatory restrictions and practical constraints affecting cooperation.
What is not changing	The reform would preserve the responsible-entity model. The connected entity would not become the responsible entity for the asset and would not assume the full CIRMP obligation set. The duty would support, not transfer, the responsible entity's CIRMP responsibility. The responsible entity would remain accountable for the CIRMP, while the connected entity would be accountable only for its own cooperation duty.

Preliminary Impact Analysis

This measure is likely to result in some parent companies, shared-services entities, subsidiaries and other related bodies corporate becoming subject to a targeted duty to cooperate, where a responsible entity materially depends on them to comply with its CIRMP obligations. The duty would follow the dependency, so corporate groups that centralise security, IT or procurement functions are the most likely to be affected.

The main costs would arise from identifying material corporate-group dependencies, updating internal governance and escalation processes, documenting cooperation arrangements, responding to reasonable requests for assistance, and notifying material events that may affect the responsible entity's compliance. Where a relevant function is controlled elsewhere in the group, the measure would make that dependency visible and manageable rather than establish a separate compliance program.

For many groups the measure may reduce compliance friction, by providing the responsible entity with a clear line to the related entities that control relevant functions. The measure is not expected to adversely affect competition, innovation or market entry.

Consultation questions

87. Is material CIRMP dependency the right trigger for a statutory cooperation duty on connected entities within a corporate group? What guidance or examples would help responsible entities and connected entities identify when a dependency is material?

88. Are the proposed limbs of the duty appropriate: not frustrating compliance, assisting on reasonable request, and notifying material incidents, changes or circumstances? Should any limb be narrowed or expanded?

89. Does the reasonableness qualifier provide an appropriate basis for proportionality, including for the nature of the dependency, the connected entity's role and capability, the burden of assistance, confidentiality obligations, foreign law constraints or regulatory restrictions?

90. Should the existing compliance and enforcement framework, including infringement notices, enforceable undertakings, injunctions and civil penalty proceedings, apply to breach of the connected entity duty? What penalty setting would be appropriate?

91. Are there practical issues in applying this framework to foreign-connected entities or groups with complex offshore ownership and control structures? How should those issues be managed?

Measure 19 – Supply Chain Cyber Security Assurance

The problem

Critical infrastructure entities increasingly depend on suppliers and service providers for the products, services, systems and access that underpin the operation of their assets. These relationships include managed service providers, software and platform vendors, cloud and hosting providers, operational

technology vendors, original equipment manufacturers, specialist integrators, offshore support centres, firmware providers and software component suppliers.

This has materially changed the cyber risk profile of critical infrastructure. Adversaries increasingly target suppliers as a pathway to the assets their customers operate. Compromise of a trusted product, software update, remote support channel, privileged credential, managed service or third-party platform can affect multiple critical infrastructure entities at the same time. Ransomware, malicious software updates, credential theft, exploitation of unpatched vulnerabilities, insecure supplier practices and abuse of privileged remote access are recurring patterns.

A responsible entity can have strong internal cyber controls and still be exposed to material cyber risk through the products it buys, the services it relies on, and the access it grants to suppliers. The cyber security posture of major suppliers is part of the asset's risk picture.

The CIRMP framework already requires responsible entities to manage supply chain hazards. Current CIRMP settings address major suppliers, privileged access, supply-chain disruption, failure or lowered capacity of supply-chain assets and entities, supplier mapping, critical systems, maximum tolerable outage, jurisdictional exposure, foreign ownership, control or influence, supplier access, influence and control, and material risk.

The gap is that the framework does not yet clearly explain what responsible entities should do to assess cyber risks from major suppliers. This includes risks arising from supplied products and services, cyber security measures built into those products and services, and supplier practices such as secure development, patching, vulnerability management, secure update mechanisms, incident notification and privileged access management.

There is also a practical assurance problem. Responsible entities and suppliers may repeat bespoke assessment processes that ask materially similar questions in different formats. This can be burdensome for suppliers, especially small and medium enterprises, and can reduce the incentive to invest in recognised cyber security uplift. A recognised certification or accreditation pathway could give responsible entities a more efficient way to evidence supplier cyber due diligence, where the certification is current, relevant and appropriately scoped.

Supplier cyber assurance also needs to be workable in specialised and concentrated supply chains. Some responsible entities rely on proprietary operational technology, specialist industrial equipment, international platforms, limited-market software or suppliers that cannot readily be replaced. In those circumstances, prescribed contractual terms or standardised assurance requests may be difficult to obtain. The framework should support documented exceptions and alternative controls where supplier constraints exist, while still requiring the responsible entity to understand and manage material residual cyber risk.

These issues can make supplier cyber assurance inconsistent, duplicative and difficult to apply in practice. Responsible entities may not have clear expectations about which major suppliers warrant cyber-specific assessment, what matters should be considered, when certification or accreditation can be relied on, and how residual risks and exceptions should be recorded and reviewed.

> **Proposed model for consultation:** Clarify how the CIRMP framework should address cyber-specific assurance for major suppliers and service providers.
>
> The intended outcome is that responsible entities would assess and manage cyber risks arising from major suppliers whose products, services, access or role are material to the security, availability, integrity, reliability or operation of a critical infrastructure asset.

The model would build on existing and recently-enhanced CIRMP supply-chain settings. Those settings address matters such as supplier mapping, major supplier dependency, foreign ownership, control or influence, jurisdictional exposure, supplier access, influence and control, and outage consequence. The additional cyber-specific focus would address:

- the quality and resilience of products and services supplied by major suppliers
- cyber security risk-management measures embedded in those products and services; and
- supplier cyber security practices, including secure development, maintenance, patching, vulnerability management, secure update mechanisms, privileged or remote access controls, incident notification and support arrangements.

Supplier cyber assurance would remain an obligation of the responsible entity through the CIRMP framework. Suppliers would not become directly regulated under SOCI by reason of this measure. Responsible entities would manage supplier cyber assurance through governance, procurement, contracting, technical controls, risk management, assurance, monitoring and review.

The framework would support contractual or equivalent measures with direct major suppliers where reasonably practicable. Equivalent measures could include documented commercial, procurement, technical, operational or assurance arrangements where formal contractual terms cannot reasonably be obtained. The approach would apply prospectively at appropriate commercial touchpoints, such as contract entry, renewal or material variation.

The framework would also support recognition of cyber security certification or accreditation as evidence relevant to supplier cyber due diligence. Recognised certification or accreditation could be relied on where it is current, relevant and appropriately scoped to the supplier, product, service, environment or risk context. Reliance on certification or accreditation would support due diligence and would not remove the responsible entity's need to consider residual, asset-specific supplier cyber risks.

The framework would recognise that material cyber risk may arise from sub-tier dependencies. Responsible entities would consider sub-tier risks where those risks materially affect the cyber risk presented by a direct major supplier or service provider. The model would not require responsible entities to identify, assess or contract directly with every supplier in the chain.

The detailed implementation pathway could involve amendments to the CIRMP Rules, recognition instruments, guidance, or Act amendments if needed. Consultation is directed to the intended outcome, proportionality settings, assurance pathways and practical implementation issues.

Key design elements

Element	Description
Supplier cyber assurance outcome	Responsible entities would be expected to assess and manage cyber risks from major suppliers and service providers whose products, services, access or role are material to the security, availability, integrity, reliability or operation of a critical infrastructure asset.

Element	Description
Major suppliers	The framework would continue to focus on major suppliers and service providers whose products, services, access, role or dependency are material to the asset's risk profile. Relevant relationships may include managed service providers, cloud and hosting providers, operational technology vendors, software and platform providers, OEMs, remote support providers, specialist integrators and comparable service providers. Contract value or commercial size would not be determinative on its own.
Cyber security assessment	Responsible entities would assess and take into account cyber risks arising from major suppliers and service providers. Relevant matters may include the quality and resilience of supplied products and services, embedded cyber security measures, supplier cyber security practices, secure development, maintenance, patching, vulnerability management, secure update mechanisms, privileged or remote access controls, incident notification and support arrangements. The assessment would be proportionate to the supplier's role, access and criticality to the asset.
Contractual or equivalent measures	Responsible entities would be expected to address supplier cyber risk through contractual or equivalent measures with direct major suppliers where reasonably practicable. The expectation would apply prospectively at appropriate commercial touchpoints, such as contract entry, renewal or material variation. It would allow for different measures across different suppliers, products and services. Equivalent measures could include documented commercial, procurement, technical, operational or assurance arrangements that manage the relevant supplier cyber risk where formal contractual terms cannot reasonably be obtained.
Recognised certification or accreditation	The framework would support recognition of cyber security certification or accreditation as evidence relevant to supplier cyber due diligence. Recognition would be scheme-agnostic and criteria-based. Relevant criteria may include independence, scope, currency, assurance rigour, renewal requirements, treatment of material changes, and suitability for the relevant supplier, product, service, environment or risk context. A responsible entity could rely on recognised certification or accreditation to the extent it is current, relevant and appropriately scoped. Reliance would support due diligence and would not displace asset-specific supplier cyber risk management.
Recognition pathway	Cyber security certifications or accreditations could be recognised through a flexible recognition mechanism, such as a notifiable instrument, Rules setting or other appropriate mechanism. This would allow existing and future Australian,

Element	Description
	international, Commonwealth or sector-specific schemes to be recognised without naming particular schemes in the Act itself.
Assurance and record-keeping	The CIRMP would record the outcomes of supplier cyber assessments, any contractual or equivalent measures in place, and the basis on which recognised certification or accreditation has been relied on. Where material residual supplier cyber risks remain, the CIRMP would record how those risks are being managed through alternative controls, mitigations, monitoring, governance or review.
Supply chain constraints and documented exceptions	Where particular contractual, assurance or equivalent measures cannot reasonably be obtained, the responsible entity would manage the relevant cyber risk through its CIRMP. This would operate as a documented exception process. The responsible entity would record the supplier constraint, why the relevant measure could not reasonably be obtained, the residual cyber risk, any alternative controls or mitigations adopted, the governance oversight applied, and when the exception will be reviewed.
Sub-tier dependencies	The framework would recognise that material cyber risk may arise from other levels of the supply chain. Responsible entities would consider sub-tier risks where they materially affect the cyber risk presented by a direct major supplier or service provider. The reform would not require responsible entities to identify, assess or contract directly with every sub-tier supplier.
Interaction with CIRMP reforms	The measure would operate alongside existing and recently-enacted CIRMP supply-chain hazard requirements. It would add a cyber-specific supplier assurance focus concerning the quality and resilience of supplied products and services, embedded cyber security measures, and supplier cyber security practices. The detailed implementation pathway could involve CIRMP Rules amendments, recognition instruments, guidance, or Act amendments if needed to support the preferred design.
What is not changing	The responsible entity would remain the regulated party. Supplier assurance would be managed through the responsible entity's governance, procurement, contracting, risk management and assurance practices. The reform would not create a new regulated supplier class. It would not require responsible entities to terminate existing suppliers, renegotiate all existing contracts, impose identical cyber terms across all suppliers, or obtain assurance that is disproportionate to the supplier's role, access and criticality.

Preliminary Impact Analysis

This measure is likely to increase regulatory costs for responsible entities that rely on major suppliers for systems, services or functions material to the security or resilience of a critical infrastructure asset. It may also indirectly affect major suppliers that are asked to provide cyber security assurance, contractual commitments or certification evidence. Exposure would vary with supplier concentration, with the greatest exposure for entities that depend on a small number of major suppliers.

The main costs arise from identifying major suppliers, assessing their cyber security risk, updating contracts or equivalent controls, reviewing certification or accreditation evidence, documenting exceptions where assurance cannot reasonably be obtained, and considering material sub-tier cyber risks through the direct supplier assessment. Where suppliers already hold recognised certifications or accreditations, entities would be able to rely on them, which reduces the incremental cost.

The effect on competition and market entry is expected to be limited because the measure would remain focused on major suppliers and allow practical alternatives where bespoke assurance or contract terms cannot reasonably be obtained. The principal risk relates to supplier concentration, including smaller, specialised or difficult-to-replace suppliers, and sectors served by a small number of suppliers. In those cases, assurance requirements could fall heavily or reduce the available supplier pool.

Consultation questions

92. Is a cyber-specific supplier assurance expectation a clear and workable addition to the CIRMP framework? What practical outcomes should responsible entities be expected to demonstrate?

93. What features should determine whether a supplier or service provider warrants cyber-specific assessment, including role, access, dependency, substitutability and effect on the security, availability, integrity, reliability or operation of the asset?

94. What supplier cyber security matters should responsible entities assess, including product and service resilience, secure development, maintenance, patching, vulnerability management, secure update mechanisms, privileged or remote access controls, incident notification and support arrangements?

95. How should responsible entities address supplier cyber risk through contractual or equivalent measures, including at contract entry, renewal or material variation?

96. What criteria should apply before a cyber security certification or accreditation scheme is recognised for SOCI supplier assurance purposes, and when should recognised certification or accreditation provide sufficient evidence of supplier cyber due diligence?

97. How should the framework deal with specialised, proprietary, concentrated or difficult-to-replace suppliers, and with material risks arising from sub-tier dependencies, without requiring responsible entities to assess or contract directly with every supplier in the chain?

98. What downstream impacts could the proposed supplier cyber assurance model have on small and medium enterprises in critical infrastructure supply chains, and what guidance, phasing or recognition pathways would reduce unnecessary duplication?

Measure 20 – Specified Risk Information

The problem

Government agencies, standards bodies and other relevant organisations routinely publish material that may be directly relevant to the security and resilience of critical infrastructure. This includes threat advisories, risk assessments, standards, hazard material and guidance that may bear on the operation, availability, integrity or security of regulated assets.

The SOCI framework does not currently provide a consistent statutory mechanism for connecting specific, relevant published risk information to a responsible entity's formal CIRMP governance, review and assurance processes. A responsible entity may be aware of relevant material, or the material may be publicly available, although there is no clear obligation to assess whether specified material changes the asset's risk profile, identifies a material vulnerability or control gap, or requires a documented response through the entity's CIRMP.

This can leave a gap between published risk information and the entity's formal risk-management processes. Important material may be available, but there may be no clear requirement for the entity to consider it, decide whether it is relevant to the asset, and record what action, if any, is needed. This can also make assurance harder. Responsible entities, boards and regulators may not have a clear record showing whether specific risk information has been considered and how the entity responded to it.

The problem is not that every advisory, standard or guidance document should automatically apply to every responsible entity. The problem is that, where specific material is directly relevant to a sector, asset class or entity, the current framework does not provide a clear and consistent way to bring that material into CIRMP governance, review and assurance.

Any mechanism would also need to avoid creating an open-ended obligation to monitor all published guidance, advisories, standards or risk material. Without clear limits, the obligation could become difficult to apply and disproportionate to the risk being managed.

> **Proposed model for consultation:** Create a targeted mechanism for the Secretary to identify specific published risk, hazard, standards or guidance material that responsible entities must consider through their CIRMP governance, review and assurance processes.
>
> A notice would identify the document or class of document, the sectors, asset classes or entities to which it applies, the date from which the obligation applies, and how the material may be accessed. The notice would identify the material rather than reproduce it.
>
> Specified material would need to be accessible to affected responsible entities and capable of being understood and considered in the context of the relevant asset, sector or risk. Supporting material, plain-language summaries, sector-specific examples or implementation guidance may be provided where the specified material is technical, complex or directed to a particular threat or sector context.
>
> The obligation would be procedural and documented. A responsible entity would be required to consider the specified material, assess whether it is relevant to the asset and its operating context, determine whether it identifies a material risk, vulnerability, control gap or governance issue, and record an appropriate response. Where the material identifies a relevant risk or gap, the entity would consider whether its CIRMP, controls or related governance arrangements should be updated. Where the entity determines that no update is required, it would record the basis for that decision.

Specified material would inform CIRMP governance and assurance without becoming automatically binding merely because it has been identified under this mechanism. The measure would apply only to material specified through the statutory process, rather than creating a general obligation to monitor all available guidance.

Where specified material overlaps with another law, regulatory requirement or lawful direction applying to the responsible entity, the entity would document the interaction, identify any legal or operational constraint, and determine a lawful and proportionate response to the underlying risk.

The policy intent is to ensure that specific, relevant risk information is considered and documented through existing CIRMP processes, without turning that material into a binding technical standard or creating a general duty to monitor all published risk material.

Key design elements

Element	Description
Notice mechanism	The Secretary would specify relevant published material by notice. The notice would identify the document or class of document, the sectors, asset classes or entities to which it applies, the date from which the obligation applies, and how the material may be accessed. The notice would identify the material rather than reproduce it.
Specified and targeted material	The mechanism would apply only to material specified through the statutory process. The material would need to be relevant to the security or resilience of the specified sector, asset class or entity. This may include published risk assessments, threat advisories, hazard guidance, standards, good-practice material or sector-specific guidance, whether published by the Department, another Commonwealth agency, standards bodies or other appropriate sources. General guidance, advisories or standards would not trigger the obligation unless specified through the notice mechanism.
Accessibility and interpretability	Specified material would need to be accessible to affected responsible entities without unreasonable barriers. In deciding whether material is appropriate to specify, regard would be had to whether the material is available, understandable and capable of practical consideration by the entities to which it applies. Supporting information, plain-language summaries, sector-specific examples or implementation guidance may be needed where the material is technical, complex or directed to a particular threat or sector context. Notices should allow reasonable time for affected entities to consider and respond to the material.
Procedural obligation only	Responsible entities would be required to consider the specified material, assess whether it is relevant to their asset and operating context, determine whether it identifies a material risk, vulnerability, control gap or governance issue, and record an appropriate response. The obligation would require documented consideration of the material's implications, with the level of analysis proportionate to the material, the asset and the relevant risk.

Element	Description
Response through existing CIRMP processes	Where specified material identifies a relevant risk or gap, the responsible entity would consider whether its CIRMP, controls or related governance arrangements should be updated. Where the entity determines that no update is required, it would record the basis for that decision. This would allow specified risk information to be considered through existing CIRMP governance, review and assurance processes.
Interaction with other obligations	Where specified material overlaps with another law, regulatory requirement, licence condition, contractual obligation or lawful direction, the responsible entity would document the interaction, identify any legal or operational constraint, and determine a lawful and proportionate response to the underlying risk.
Assurance and reporting	The framework would support assurance by allowing Government to ask whether specified material has been considered and how the entity responded. This could occur through the broader CIRMP review, reporting and assurance architecture. A responsible entity would be expected to demonstrate that it considered applicable specified material, assessed its relevance to the asset and operating context, and recorded a reasoned response.
What is not changing	The reform would not convert specified material into a binding technical standard merely because it has been identified under this mechanism. It would not require automatic adoption of every recommendation in a specified document. It would require responsible entities to consider specified material, assess its relevance, and document their response through existing CIRMP processes.

Preliminary Impact Analysis

This measure would impose a modest, procedural obligation on entities subject to CIRMP obligations, requiring them to consider specified risk information and document how it has been taken into account. It would require entities to engage with the material, rather than to adopt any particular control.

The main costs would arise from reviewing the material, assessing its relevance to the entity's risk environment, documenting a reasoned response, and updating CIRMP controls where the entity identifies a need to do so. These costs would vary with the volume, frequency, specificity and accessibility of the material specified by the Secretary. Well-curated and clearly presented material would reduce the cost of consideration. The measure is not expected to adversely affect competition, innovation or market entry, because the information would not be binding and would not impose a uniform technical standard.

Consultation questions

99. Is a procedural obligation to consider specified published risk information and record a response the right calibration?

100. What kinds of published documents should be capable of being specified, and what categories should be excluded from the mechanism?

101. What would be a workable way for responsible entities to document consideration of specified material through existing CIRMP governance, review and assurance processes?

102. What safeguards are needed to ensure specified material informs risk management without becoming a de facto prescriptive control list?

103. What accessibility, timing, notification or guidance settings are needed so affected entities can reasonably comply once material is specified?

104. How should the framework operate where specified material overlaps with another legal, regulatory, contractual or operational requirement?

Measure 21 – Critical Workers and Critical Components

The problem

The current definition of a critical worker is difficult to apply consistently and does not provide a clear basis for proportionate personnel-security obligations. It relies heavily on consequence-based judgments by the responsible entity, including whether a person's absence or compromise would prevent proper function of the asset or cause significant damage. It also links critical worker status to the separate concept of a critical component, which can make the definition circular in practice.

This creates uncertainty for responsible entities and workers. Entities must identify critical workers, manage personnel hazards, apply suitability and background checking settings, and control access to critical components, yet the current definition gives limited objective guidance about which roles, access profiles or forms of authority should be treated as security sensitive.

The current framework also does not align well with contemporary operating models. Access to critical systems, facilities, information and operational decision-making may be exercised by personnel working for relevant operators, connected entities, managed service providers, OEMs, contractors or other third parties. A definition focused in practice on the responsible entity's own workforce may miss people whose role, access or authority is material to the operation, availability, integrity or security of the asset.

The current framework is also too binary. It identifies a single class of critical worker and does not provide a sufficiently clear basis for applying different personnel-security obligations to different kinds of role, access or authority. A person with privileged administrative access to operational technology, a person with unescorted access to a restricted security-critical area, and a person with operational authority over a critical function may present different levels and types of risk.

The policy problem is that the current definition does not give responsible entities a clear, objective and proportionate way to identify workers whose role, access or authority creates personnel-security risk. This can make the framework harder to apply, particularly for contractors and third-party personnel, and can result in similar controls being applied to roles that present different levels of risk.

Proposed model for consultation: Replace the current critical worker definition with a clearer access-based and authority-based definition. The new definition would preserve the critical worker concept as the operative gateway for the existing personnel-security framework and would apply to work performed in connection with a critical infrastructure asset to which the personnel-security settings apply.

The proposed definition would identify critical workers by reference to specified security-sensitive roles, access, authority, control, management or information holdings. It would be capable of applying to personnel of the responsible entity and to personnel of relevant operators, connected entities, managed service providers, contractors and other third parties, where their role, access or authority meets the statutory and Rules-based criteria.

The proposed model would operate through four alternative categories:

- security-sensitive access
- operational authority
- access to a critical component; and
- prescribed roles.

A person would only need to satisfy one category to be a critical worker. The Rules would then be able to prescribe different obligations, controls or checking requirements for different classes of critical worker, calibrated to the nature and degree of risk.

The critical component definition would also be refined. The Act would retain a core concept of critical component, and the Rules would be able to prescribe kinds of components, systems, environments, facilities or other parts of an asset that are to be treated as critical for particular sectors, asset classes or circumstances. The Act would retain a residual test for components whose disruption, compromise or unavailability would materially affect the operation, availability, integrity or security of the asset.

The responsible entity would remain responsible for identifying which roles or persons fall within the critical worker framework for its asset. That assessment would be based on statutory and Rules-based criteria, with a focus on roles, functions and access profiles rather than broad, ad hoc person-by-person judgment.

The reform is intended to confine the critical worker concept to specified security-sensitive roles, access, authority or functions that are materially relevant to the operation, availability, integrity or security of the asset or its critical systems and components. It is not intended to bring the general workforce into scope.

Key design elements

Element	Description
Gateway condition and broader workforce nexus	The concept would continue to operate as the gateway for the existing personnel-security framework. The relevant nexus would be work performed in connection with a critical infrastructure asset to which the personnel-security settings apply. The concept would be capable of applying to personnel of the responsible entity and to personnel of relevant operators, connected entities, managed service

Element	Description
	providers, contractors and other third parties, where their role, access or authority meets the statutory and Rules-based criteria.
Critical worker criteria	A person would be a critical worker if they satisfy one of four alternative limbs: security-sensitive access, operational authority, access to a critical component, or a prescribed role. This would give the Act a clearer and more objective structure while preserving flexibility for sectoral calibration through the Rules.
Security-sensitive access and operational authority	The new model would give greater weight to objective indicators of security sensitivity. These may include privileged or administrative access to operational technology, industrial control systems, identity and access management systems, network management systems, safety-related systems or other security-critical systems. They may also include access to security-sensitive information about the asset, including information about design, configuration, vulnerabilities, dependencies or security arrangements; unescorted access to restricted security-critical areas; installation, configuration, integration, testing, maintenance, patching or updating of security-critical systems; and authority to operate, configure, maintain or materially influence critical functions or systems.
Reformed critical component concept	The critical component definition would be retained and refined. The Act would retain the core concept of a part of the asset, or a part of the systems or infrastructure used for the asset, whose disruption, compromise or unavailability would materially affect the operation, availability, integrity or security of the asset. The Rules would be able to prescribe kinds of components, systems, facilities, environments or other parts of an asset that are to be treated as critical for different sectors, asset classes or circumstances. A residual Act-level test would remain for components that are not prescribed in the Rules but are objectively material to the operation, availability, integrity or security of the asset.
Role-based identification and documentation	Responsible entities would continue to identify which roles or persons fall within the critical worker framework for their asset. They would do so by applying criteria set by the Act and Rules. The identification process would focus on roles, functions and access profiles. Responsible entities would document the categories of roles treated as critical worker roles through their CIRMP personnel hazard settings and related internal processes.
Proportionate obligations through the Rules	The Rules would be able to distinguish between categories of critical worker and apply different obligations, controls or restrictions according to risk. This may include different suitability assessment, background checking, monitoring, supervision, training or access-control requirements. This would allow higher-risk roles or access profiles to attract stronger controls, and lower-risk categories to be managed through lighter-touch settings.

Element	Description
Transition	Responsible entities would be given a reasonable period to review and re-identify critical worker roles and categories under the amended definition and update their CIRMP personnel hazard settings and related internal processes. Individuals identified as critical workers under the existing framework could continue to be treated as satisfying relevant pre-commencement requirements for a transitional period, or until the responsible entity completes its review. Existing background checks or suitability assessments would continue to be recognised where they remain current under the Rules. Further checks would be required only where a role is reclassified into a higher-risk category, a previous check is no longer current, or another prescribed trigger applies.
What is not changing	The reform would retain the critical worker concept and preserve its role in the existing Part 2A and CIRMP personnel-security architecture. The reform would not bring the general workforce into scope. Detailed obligations would continue to be calibrated through the Rules, so personnel-security controls can be matched to the role, access or authority that creates the risk.

Preliminary Impact Analysis

This measure would require responsible entities to reassess which workers, contractors and third-party personnel are treated as critical. The model would move from the current consequence-based definition to clearer access-based and authority-based criteria. The clearer definition is expected to reduce uncertainty over time, although the initial reassessment would fall most heavily on entities with large or distributed workforces.

The main costs arise from role mapping, access and authority assessment, updating personnel-security procedures, identifying critical components, and applying any Rules-prescribed checking, monitoring, training, supervision or access-control requirements. Costs are expected to be higher for entities with large contractor workforces, outsourced operational functions, managed-service arrangements or complex access-control environments. The initial role-mapping exercise is expected to be the principal one-off cost.

The measure is not expected to materially affect competition, innovation or market entry where Rules settings are calibrated to roles that create genuine personnel-security risk. The impact would depend on how the role categories and critical-component settings are defined, particularly for smaller responsible entities and those operating distributed workforces, for which broad settings could result in disproportionate implementation costs.

Consultation questions

105. Does an objective, access-based and authority-based definition better identify the people whose role, access or authority gives rise to personnel-security risk for critical infrastructure assets?

106. What kinds of security-sensitive access, operational authority, information holdings, systems, facilities or locations should be specified in the Act or Rules?

107. Does the proposed approach to critical components provide a workable balance between an Act-level concept and Rules-based specification for different sectors, asset classes and circumstances?

108. Which categories of third-party personnel should be capable of falling within scope, including personnel of relevant operators, connected entities, managed service providers, contractors or other third parties? Which categories should remain outside scope?

109. How should the Rules differentiate obligations for different classes of critical worker, including suitability assessment, background checking, monitoring, supervision, training and access-control settings?

110. What transition period, guidance and implementation support would responsible entities need to re-identify critical worker roles and update CIRMP personnel hazard settings?

111. What number and proportion of workers may be captured under the proposed revised definition, including direct employees, contractors, relevant operator personnel, connected entity personnel, managed service provider personnel and other third-party workers?

Appendix A – Independent Review recommendation mapping

This Appendix maps the recommendations of the Independent Review, including the issues identified under Recommendation 6(a), to the Government's response pathway. It shows how those recommendations are being progressed across Tranche 1 reforms, the Tranche 2 measures in this paper, related Rules work, guidance and future implementation activity. It should not be read as requiring a one-to-one correspondence between each recommendation and a single legislative measure. In many cases, the Government's response spans multiple workstreams and will continue to be refined through further consultation.

Review Recommendation	Government response pathway
Recommendation 1: Remove duplication and improve harmonisation	Progressed through a linked reform program across both tranches. Tranche 1 includes work to better align SOCI settings with related transport-security and CIRMP reforms. Tranche 2 advances broader anti-duplication reform, including the proposed exemptions framework and other streamlining measures intended to reduce overlap where another Commonwealth, State or Territory law, or another recognised framework, already imposes substantially equivalent or stronger requirements. Implementation work will continue with industry and other regulators to identify practical overlap and develop workable forms of relief.
Recommendation 2: Move from light-touch compliance to stronger enforcement	Progressed through both tranches. Tranche 1 includes stronger civil penalties for non-compliance with Ministerial directions and reforms to improve the operability of intervention powers. Tranche 2 strengthens the broader compliance and assurance architecture through redesigned reporting, stronger CIRMP governance and review requirements, mandatory independent assurance, register reform, improved information-gathering tools, and a targeted recalibration of selected civil penalty settings for core preventive and assurance duties. The Department will also continue to examine non-legislative compliance and assurance settings so that the framework is supported by effective implementation, supervision and enforcement.
Recommendation 3: Develop Australian Securities and Investment Commission (ASIC)-style regulatory guides with worked examples	Progressed primarily through a continuing administrative guidance and implementation workstream accompanying both tranches. This will include clearer sector-specific materials, worked examples, templates and supporting guidance to improve clarity, support practical compliance and reduce unnecessary complexity. This work forms part of the Government's broader future program to simplify and rationalise the framework and will be developed with industry.
Recommendation 4: Respond to emerging technologies and threats	Progressed through both tranches. Tranche 1 includes CIRMP and Directions reforms directed to urgent vendor, FOCI, advanced

Review Recommendation	Government response pathway
	technologies, cyber and intervention-related risks. Tranche 2 further modernises the framework by addressing sector and asset gaps and contemporary operating models, including reforms relating to space technology, data infrastructure, distributed energy resources, offshore electricity, higher education and research, supply-chain cyber security and cyber security incidents involving automated systems, software agents and AI-enabled tools.
Recommendation 5: Enhance TISN capability through education and information sharing	Progressed through non-legislative implementation work, including Government-led engagement with industry, education and information-sharing activities, supported by targeted legislative measures that improve the framework's practical operation, guidance and capability uplift. This includes work on specified-risk-information mechanisms, clearer guidance materials, and future co-designed implementation support.
Recommendation 6: Accept CIRMP amendments while working toward simplification and rationalisation of the SOCI Act	Progressed through two linked stages and a continuing future workstream. Tranche 1 addresses urgent intervention and risk-management gaps through CIRMP Rules uplift and reforms to the Ministerial directions framework. Tranche 2 advances broader simplification, anti-duplication, structural reform, coverage modernisation and strengthened assurance architecture within the existing framework. These stages will be followed by a continuing program of simplification and rationalisation, including ASIC-style regulatory guides, worked examples and co-designed implementation materials. That future work will support a clearer and more principles-based future framework over time.
Recommendation 6(a)	
Definitions	Progressed through multiple measures in this paper, including reforms relating to space technology, distributed energy resources, offshore electricity assets, higher education and research, healthcare and medical sector coverage, freight, operations and maintenance providers, corporate group cooperation, and critical workers and critical components. These measures address a substantial part of the gaps and ambiguities in sector, asset and responsibility settings identified by the Review. Other perimeter or calibration issues do not necessarily require Act-level amendment and may be addressed through subsequent Rules amendments, exemptions, sector-specific calibration or further targeted reform where warranted.
Register of CI Assets	Progressed through the Register of Critical Infrastructure Assets reform within the broader compliance and assurance uplift in this paper, including broader statutory information categories, simpler notification settings, and a proposed category for targeted systems, suppliers and dependencies information.

Review Recommendation	Government response pathway
Information sharing mandate	Progressed in part through the specified-risk-information proposal in this paper. Broader work on engagement, education and information sharing with industry will continue alongside legislative reform. Broader two-way information-sharing issues are not fully resolved in this tranche and may require further policy consideration or future reform.
Risk management programs	Progressed through both tranches. The CIRMP enhancement program proposed uplift across all-hazard, cyber, supply-chain and personnel-security settings for specified high-risk asset classes. This paper further strengthens the CIRMP architecture through stronger governance controls, clearer review and currency requirements, mandatory independent assurance, and related compliance reforms. Some matters raised in the Review, such as whistleblower protections, are not specifically progressed in this paper and may require further policy consideration.
Incident reporting	Addressed in part in this tranche. Measure 5 would refine the Act-wide definition of “cyber security incident”, which supports Part 2B reporting and other operative provisions that use that term. This paper does not propose a wholesale redesign of the broader incident-reporting framework. Further work may be required on issues raised by the Review about wider outage and all-hazards reporting settings.
TISN compliance	Not implemented as a specific legislative measure in this paper. It remains relevant to broader administrative and capability work associated with TISN engagement, education, implementation support and information sharing.
Systems of National Significance	Progressed through the SoNS reform package in this paper, including clearer consequences of designation, asset-specific resilience planning, cyber security exercises, discretionary all-hazards vulnerability assessments, repeal of the System Information ECSO, and clearer recognition of equivalent arrangements.
Ministerial Directions	Progressed through the separately consulted Tranche 1 reforms to the Ministerial directions framework in Part 3, including amendments to section 32, a conditions power, a vendor-risk directions power, a delayed continuous-disclosure mechanism, and stronger civil penalties for non-compliance with directions.
Hosting certification	Progressed in part through the data storage or processing reform package in this paper, including certification-based capture through the Hosting Certification Framework or equivalent schemes, and through related work on exemptions and overlap settings. Further work on the broader legal framework surrounding certified hosting arrangements is being progressed separately.
Assets under construction	A dedicated measure focused on pre-operational security for assets under construction is not included in this consultation paper. The Government is

Review Recommendation	Government response pathway
	seeking views on whether further SOCI reform may be needed to address high-risk pre-operational projects, and how any such reform should interact with existing project approval processes, foreign investment settings, procurement frameworks, sector-specific regulation and ordinary SOCI obligations that apply once an asset becomes operational. One possible approach would be to focus any future SOCI coverage on a targeted class of high-criticality projects where security risks introduced during design, procurement, construction or commissioning could be difficult or impossible to remediate once the asset is operational. Any future model would need clear criteria, procedural safeguards, proportionate obligations, appropriate transition points between pre-operational and operational obligations, and mechanisms for Government to identify relevant projects without creating unnecessary investment uncertainty.
High-risk vendors	Progressed through the vendor-risk directions proposal in the separate Part 3 directions reform program, and through supply-chain and vendor-of-concern measures proposed in the CIRMP enhancement program.
Information sharing protections and best-practice sharing	Not fully resolved in this paper. Related issues are addressed indirectly through specified-risk-information reform, broader guidance work, and the Review's simplification agenda, but further work may still be needed on Part 4 and related protected-information settings.
Energy sector	Progressed through the distributed energy resources reforms and offshore electricity reforms in this paper, together with the broader cyber, supply-chain and FOCI-related proposals consulted on through the CIRMP enhancement program.
Education sector	Progressed through the higher education and research measure in this paper, which proposes a new asset definition based on prescribed technology domains and a clearer national security nexus.
Food and grocery sector	A dedicated food and grocery sector amendment is outside the current proposed package. The Government remains open to considering whether further work is needed in this area. Stakeholders are invited to provide evidence on whether current SOCI settings adequately address nationally significant food and grocery dependencies, including any issues relating to concentration, limited substitutability, distribution, cold chain, supply-chain interdependencies, data or logistics systems, and interaction with existing food, biosecurity, transport, health or emergency management frameworks.
Self-attestation	Progressed through the compliance and assurance uplift in this paper, including mandatory independent assurance, stronger governance controls, clearer CIRMP review requirements, and improved compliance architecture.
National security concerns and authority to mandate action	Progressed through both tranches, including the proposed Part 3 directions reforms, stronger compliance and information-gathering settings in this

Review Recommendation	Government response pathway
	paper, register reform, and SoNS reform. These measures would improve the Government's ability to obtain visibility, require action, and respond earlier where national security risks arise.