SUBMISSION

Proposed amendments to streamline and modernise the Security of Critical Infrastructure Act 2018

Submission to the Department of Home Affairs

Australian Logistics Council

July 2026

Table of contents

Table of recommendations

No.	Recommendation
1	Set freight capture thresholds in the Rules using national consequences, concentration, substitutability, time to impact, and restoration time; use revenue, throughput, fleet size, and freight volume only as screening indicators.
2	Set the principal freight asset classes and thresholds in the Rules, reserve designation for exceptional or emerging risks, and provide notice, reasons, a genuine opportunity to respond, appropriate review rights and adequate transition.
3	Attach SOCI obligations to the systems, facilities and operational capabilities an entity owns, operates or materially controls; require entities to manage dependencies without assuming duties for another party's asset.
4	Apply the same consequence test across road, freight rail, maritime and aviation, and create a separate, narrowly defined pathway for nationally significant traffic and transport control systems.
5	Recognise equivalent Commonwealth, State and Territory obligations on an obligation-by-obligation basis, and publish class exemptions and deemed-compliance arrangements before new freight duties commence.
6	Complete and publish a freight-specific final Impact Analysis before settling the Rules, with costs broken down by mode, business size, location, current regulatory status and SOCI obligation, and separately assess competition, supplier capacity, and cost pass-through.
7	Permit corporate groups to use common governance, CIRMP, assurance and reporting where risks and controls are shared; reuse existing audits and controls, and limit direct duties on service providers, relevant operators, connected entities and suppliers to matters within their knowledge, authority and control.
8	Require the Government to identify any Defence or national security dependency that industry cannot reasonably know; exclude predominantly export-dedicated supply chains without a demonstrated Australian consequence and regulate only the critical component where practicable.
9	Keep governing bodies responsible for oversight rather than operational ownership of the CIRMP, preserve good-faith protections for annual compliance and assurance reporting, and confine enforcement to false or misleading reports, deliberate concealment or serious and repeated failures to remediate.
10	Publish all final instruments, thresholds, exclusions, exemptions, guidance and assurance standards before commencement; allow at least six months for assessment and registration, 18 months to implement a CIRMP and 24 months before the first independent assurance review, and impose enhanced obligations only after a separate assessment.

1. About the Australian Logistics Council

The Australian Logistics Council (ALC) is the independent, trusted voice of modern supply chains for Australia.

The ALC works closely with government and industry to shape Australia's future supply chain.

ALC members operate across the end-to-end supply chain, including freight rail, road transport, ports, airports, stevedoring, intermodal terminals, warehousing, logistics, property and technology. We focus on delivering excellent services and support to our members and, with them, driving enhanced end-to-end supply chain productivity, efficiency and sustainability for the nation.

We connect industry with governments, policy makers and regulators at all levels to ensure the needs of the sector are heard and considered in investment, policy and regulatory decisions.

2. Executive summary

ALC supports stronger critical infrastructure security in principle.

ALC supports updating the freight provisions of the *Security of Critical Infrastructure Act 2018* (the Act), however, the current definitions do not fully reflect how modern supply chains operate.

Some intermodal nodes rely on shared operational technology. A failure in one privately controlled system can disrupt several supply chains, even if that system falls outside the current Act.

ALC welcomes the Department of Home Affairs' (the Department) focus on removing duplication, clarifying asset boundaries and testing whether controls work in practice.[1] [2]

Terms such as 'nationally significant node', 'logistics platform' and 'chokepoint' are too broad as drafted. Without clearer limits, they could capture ordinary freight assets that do not warrant national security regulation.

However, industry needs to know where the line is before committing legal, technology and assurance resources.

This is because Australia's freight task is delivered through separately owned, operated and regulated functions, including ports, stevedores, road carriers, freight rail operators, rail infrastructure managers, intermodal terminals and distribution centres. Energy, telecommunications and data providers support each stage.

No participant controls the whole chain; reliance on another asset is not the same as control of it.

The Department's criticality test needs to consider consequences, concentration, available substitutes, and restoration time. Revenue, throughput, fleet size, and freight volume may help screen assets for closer assessment, but they should not serve as stand-alone thresholds.

The Government should use designation only for unusual or emerging risks. It should give the affected entity notice, reasons, a genuine opportunity to respond, appropriate review rights and enough time to comply. The reforms will not work if businesses must prove the same control twice.

ALC members already comply with aviation and maritime security laws, rail safety requirements, work health and safety duties, privacy laws, cyber security obligations, and State transport regulations - where an existing regulatory set delivers the same or a stronger result, the corresponding SOCI requirement should be treated as satisfied.

The Department has identified threshold assessment, asset and systems mapping, registration and regulatory alignment as initial costs, followed by CIRMP administration, reporting, assurance, supplier work and personnel controls. Multi-jurisdictional networks and regional operators are likely to carry a disproportionate share of that burden.[3]

Independent assurance, contract changes, systems mapping and repeated requests for evidence of existing controls will all add to industry costs.

1 Department of Home Affairs, Streamlining and Modernising the Security of Critical Infrastructure Act 2018: Consultation Paper (July 2026).

2 Security of Critical Infrastructure Act 2018 (Cth), compilation no. 9, 4 June 2026.

3 Department of Home Affairs, Streamlining and Modernising the Security of Critical Infrastructure Act 2018: Consultation Paper (July 2026).

The Government should not commence the reforms until it publishes the Act, Rules, thresholds, exclusions, exemptions, guidance, forms and assurance standards as a single package for stakeholder comment. Newly captured freight entities should first enter the baseline SOCI tier. The Government should impose enhanced CIRMP or Systems of National Significance obligations only after a later, separate assessment.

The following comments are now made.

3. Need for a mode-by-mode analysis

One threshold cannot sensibly apply to every transport mode. Road, freight rail, maritime and aviation differ in ownership, control, available alternatives and existing regulation.

As the following analysis suggests, applying the same test to all four could produce arbitrary outcomes and distort competition.

Road transport and connected transport systems

Road transport is spread across many operators, vehicles and depots, almost all using public infrastructure. Capacity can often be transferred between fleets, providers, and routes, although not always quickly enough for essential supplies or remote communities. Fleet size, national customers or revenue should not, by themselves, bring a carrier into the regime.

Capture is more likely to be justified where a concentrated capability cannot be replaced before serious consequences occur. Examples could include a highly specialised national distribution service, a uniquely placed regional operator or a business-controlled system whose loss would interrupt several nationally significant supply chains.

In road freight, the nationally significant risk may sit in the transport control system, not with the carrier using it.[4]

Ordinary roads, local traffic systems, individual vehicles, standard fleet telematics, local depots and common transport-management software should remain outside scope. A digital or control system should be considered only when it exercises material operational control at a significant scale, and there is no workable manual or alternative pathway.

Freight rail

Freight rail requires a clear line between below-rail infrastructure, above-rail operations and terminals. Different entities commonly perform these functions under access agreements, network rules and safety management systems, and one service may cross several networks and jurisdictions. Treating an entire corridor or network as a single asset would obscure who controls each risk.

Below rail may include track, signalling, train control, network communications and access systems. Above-rail covers rolling stock, crew systems, dispatch, maintenance, and operator-controlled technology. Terminals control gates, yards, loading systems and local transfer interfaces. Each may be critical. **The obligation must sit with the entity that owns, operates or materially controls the function concerned.**

Freight rail already operates under the Rail Safety National Law, including safety management systems, accreditation, occurrence reporting and interface coordination. Members have identified duplication with that framework as a material cost risk. SOCI should deal with security and all-hazards resilience gaps that rail safety law does not already address. Equivalent exercises, assurance and interface controls should be accepted rather than repeated.[5]

Modal neutrality is important. A road carrier is not responsible for the public road it uses. In the same way, an above-rail operator should not become responsible for an open-access rail network beyond its control. Incorporation of the below-rail infrastructure into SOCI, but not an equivalent/substitutable road network, will

4 Department of Home Affairs, Streamlining and Modernising the Security of Critical Infrastructure Act 2018: Consultation Paper (July 2026).

5 Office of the National Rail Safety Regulator, Interface Coordination.

negatively impact competition between modes, as costs would be incurred by one mode but not the other. **Comparable public road and rail infrastructure should be assessed on comparable terms.**

Ports, stevedoring and maritime freight

A port precinct can include the port authority, facility operators, stevedores, towage and pilotage providers, shipping lines, landside carriers, terminals and government agencies. Several of those participants and functions already fall under SOCI or maritime security legislation. The same primary function should not be recaptured under a freight label.[6][7][8]

Regulation needs to follow the function and the entity that controls it. A critical port should remain regulated as a port asset. A separately controlled landside terminal, logistics platform or distribution system may qualify as a freight asset if it meets the national-consequence test. Class-based relief should apply where maritime security plans, access controls, personnel arrangements, exercises or incident reporting already satisfy the equivalent SOCI requirement.

Ports cannot operate effectively without towage, pilotage and stevedoring. That importance, by itself, does not make every provider nationally critical.

Airports and air freight

Air freight accounts for a small share of total tonnage, yet it can be critical due to time and geography. Medicines, urgent parts, perishables, live animals and supplies for remote communities may have few practical substitutes. A regional airport or cargo capability can therefore be critical despite modest annual traffic.

Airports, aircraft operators, regulated cargo agents, known consignors and other aviation participants already operate under aviation transport security legislation. Equivalent controls should be recognised directly. An airport or cargo operator should not have to prove the same control twice to different Commonwealth regulators.[9][10]

Freight forwarders and cargo handlers should not be captured simply because they handle important goods. The threshold requires material control of a nationally significant node, system, or capability, together with the absence of timely substitutes.

Intermodal terminals and transfer points

Intermodal terminals may warrant freight regulation because they concentrate transfers between road, freight rail and ports. The current Definitions Rules already name certain intermodal transfer facilities. The new framework needs transparent criteria and a practical way to update the prescribed population, rather than another list that becomes outdated.[11]

The regulated perimeter should stop at the facilities and systems controlled by the terminal entity: gates, yards, loading systems, terminal operating systems and local interfaces. It should not run along public roads or rail

6 Security of Critical Infrastructure Act 2018 (Cth), compilation no. 9, 4 June 2026.

7 Maritime Transport and Offshore Facilities Security Act 2003 (Cth), compilation no. 31, 27 March 2026.

8 Maritime Transport and Offshore Facilities Security Regulations 2003 (Cth), compilation no. 48, 22 January 2026.

9 Aviation Transport Security Act 2004 (Cth), compilation no. 39, 27 March 2026.

10 Aviation Transport Security Regulations 2005 (Cth), compilation no. 78, 1 April 2026.

11 Security of Critical Infrastructure (Definitions) Rules (LIN 21/039) 2021 (Cth), current compilation.

networks serving the site. Criticality will depend on alternative terminal capacity, access constraints, recovery time and the consequences for essential or nationally significant supply chains.

Warehousing, distribution and cold chain

Most warehouses and distribution centres are commercial assets with some capacity to substitute inventory, labour or site operations. Size is not decisive. A large facility may be replaceable, while a smaller cold-chain site may be difficult to substitute because of location, approvals, temperature-control capability or service to an isolated region.

Capture should be confined to concentrated distribution networks or specialist nodes whose loss would cause serious national or major regional consequences before alternatives could be mobilised. Inventory buffers, alternate sites, reciprocal arrangements, mobile assets, manual workarounds and the ability to divert freight all need to be considered.

Duplicate regulation also needs to be avoided. A facility already captured for its primary role in food and grocery, health, liquid fuel, or another SOCI sector should not also be treated as a freight asset unless it performs a separate critical freight function.

Digital freight platforms and operational technology

Digital systems coordinate bookings, slots, dispatch, inventory, train paths, vehicle movements, cargo visibility and terminal operations. A single compromised platform can disrupt several operators and modes. The legal boundary should turn on operational authority, not merely on the commercial importance of the information displayed.

A platform should be captured only where it can materially control or disable a nationally significant freight function, and there is no workable manual or alternative system.

When the underlying cloud, telecommunications or data-centre provider is already regulated under another SOCI class, the freight entity should manage the dependency and contractual risk. It should not have to duplicate the provider's controls or ensure matters it cannot inspect.

Conclusion

This means the SOCI Act should remain focused on national security. Freight assets should be captured only where their disruption would have serious consequences - enough to justify ongoing Commonwealth oversight.[12] [13]

While Australia’s supply chain logistics and freight transport industry is economically important, economic scale and importance do not equal criticality. A large operator may be readily substituted. A small regional facility may be the only practical link for fuel, food, medicines or remote communities.[14] [15]

12 Security of Critical Infrastructure Act 2018 (Cth), compilation no. 9, 4 June 2026.

13 Security of Critical Infrastructure (Critical Infrastructure Risk Management Program) Rules (LIN /23/006) 2023 (Cth), compilation no. 2, 10 June 2026.

14 Bureau of Infrastructure and Transport Research Economics, Australian Infrastructure and Transport Statistics Yearbook 2025: Freight.

15 Infrastructure Australia, High Productivity Freight Networks.

Criticality cannot be judged solely by size or throughput. The assessment must examine how quickly harm would occur, whether spare capacity or alternate routes are available, how long recovery would take and whether Defence, emergency response or essential supplies would be affected.

The National Freight and Supply Chain Strategy already address the wider productivity and resilience task. SOCI reform should address the smaller set of vulnerabilities that genuinely require national security regulation, without extending to ordinary freight operations.[16]

Home Affairs should develop and test the freight criteria iteratively with industry, transport agencies and State and Territory regulators before finalising the Rules, using mode-specific worked examples to confirm that the perimeter captures genuine national vulnerabilities rather than ordinary freight activity.

16 Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts, National Freight and Supply Chain Strategy and 2025-29 National Action Plan.

4. Regulatory burden and costs to industry

This means the regulatory burden resulting from a further level of regulation needs to be considered.

Poorly designed regulation consumes the same people and budgets needed to manage real security risks. Time spent reconciling overlapping laws, repeating assurance and producing the same evidence for several regulators leaves less capacity for operational technology, physical security, incident response and recovery.

The practical test is whether the reforms reduce duplication and improve security. Dr Jill Slay AM, Independent Review of the Security of Critical Infrastructure Act 2018: Final Report (Review) drew 50 submissions, 89 survey responses and roundtables involving more than 600 participants.

About 70 per cent of recorded sentiment described the SOCI framework as complex, confusing or duplicative. More than half of the survey respondents reported overlap with other regulatory systems. The Review recommended removing Commonwealth duplication wherever possible.[17]

In particular:

- The Business Council of Australia reported that organisations are spending heavily on interpreting scope and preparing compliance material, at the expense of incident response, recovery and supply-chain assurance.
- The Australian Institute of Company Directors made a similar point: many entities require costly external legal advice to understand the Act, and repeated amendments can produce a burden out of proportion to the benefit.[18] [19]
- Transport for NSW identified duplicate State and Commonwealth reporting, broad definitions and uncertainty where an asset falls into more than one category. National freight networks face exactly those conditions.[20]
- The Australian Small Business and Family Enterprise Ombudsman gave the example of an eight-person regional managed service provider facing about $40,000 in initial governance costs and 1.5 days of owner time each week to meet demands passed down by a regulated customer.
- At the Office of Impact Analysis, with a default labour rate of $85.17 an hour, the time cost alone is about $50,000 a year, before technology, certification, assurance, and legal expenses. It is not a freight-sector average, but it shows how quickly contractual flow-down can overwhelm a small regional supplier.[21] [22]
- AICD also referred to research estimating that federal regulatory compliance rose from 4.2 per cent of GDP in 2013 to 5.8 per cent in 2025, and while the ALC does not use that figure as an estimate of SOCI

17 Dr Jill Slay AM, Independent Review of the Security of Critical Infrastructure Act 2018: Final Report (tabled 24 March 2026).

18 Business Council of Australia, Submission to the Independent Review of the Security of Critical Infrastructure Act 2018 (December 2025).

19 Australian Institute of Company Directors, Submission to the Independent Review of the Security of Critical Infrastructure Act 2018 (December 2025).

20 Transport for NSW, Submission to the Independent Review of the Security of Critical Infrastructure Act 2018 (December 2025).

21 Australian Small Business and Family Enterprise Ombudsman, Submission to the Independent Review of the Security of Critical Infrastructure Act 2018 (December 2025).

22 Office of Impact Analysis, Regulatory Burden Measurement Framework (1 July 2026).

costs, it does highlight the need for the Department to examine the cumulative burden on businesses already dealing with multiple regulatory systems.[23]

Poorly designed regulation consumes the same people and budgets needed to manage real security risks. Time spent reconciling overlapping laws, repeating assurance and producing the same evidence for several regulators leaves less capacity for operational technology, physical security, incident response and recovery.

The practical test is whether the reforms reduce duplication and improve security.

Costs will vary across participants in the freight and logistics industry.

Large operators will first have to work out which parts of their business are captured. For some, that means reviewing hundreds of sites, systems, contracts, entities and dependencies across several jurisdictions.

Freight rail presents a distinct boundary problem. Different entities manage above-rail operations, below-rail infrastructure, and terminals, while a single service may span several networks. Making one party reassess another regulated party's resilience adds cost without placing the risk with the party able to control it.

Ports, stevedores, airports and air-cargo participants already pay for transport security programs, access controls, ASIC and MSIC arrangements, emergency management exercises, incident reporting, audits and regulator engagement.

Example: *Road freight is dispersed and competitive. Operators often work on thin margins, under fixed or long-term contracts, using public infrastructure they do not control. Uneven treatment of comparable road and freight rail functions could affect mode choice without reducing national risk.*

Regional and specialist operators are likely to carry the highest proportional cost. Cyber, operational technology, and multidisciplinary assurance expertise are harder to source outside major cities, which increases fees, travel, and implementation time. An overly broad supplier or critical-worker definition may also shrink the pool of available regional contractors.

Operators will either absorb the cost, seek to recover it when contracts are renewed or reduce other investments. In each case, the effects will eventually reach freight customers, businesses and households.

The final Impact Analysis must reflect this variation.

Costs that sit outside the formal regulatory burden estimate

The Office of Impact Analysis Framework (Framework) requires administrative, substantive compliance and delay costs to be measured over a default 10-year period. Some opportunities and indirect costs fall outside the formal Regulatory Burden Estimate, although significant effects must still be presented.

For the supply chain logistics and freight transport industry, the analysis needs to cover:[24]

- **Reduced capital available for fleet, terminal, network, cyber and resilience investment.**
- **suppliers exit or consolidation caused by assurance and contractual flow-down;**
- **reduced competition between large and small operators and between transport modes.**
- **Higher barriers to entry for regional and specialised providers.**
- **costs passed through to freight customers and, ultimately, households and businesses; and**

23 Australian Institute of Company Directors, Submission to the Independent Review of the Security of Critical Infrastructure Act 2018 (December 2025).

24 Office of Impact Analysis, Regulatory Burden Measurement Framework (1 July 2026).

- **operational delay where approvals, assurance or contract renegotiation prevent deployment of systems or services.**

Cost control measures that could be implemented

Given this, the following reforms could be considered for adoption during the implementation process:

- **Class exemptions and deemed-compliance arrangements for equivalent aviation, maritime, rail safety and other transport regulations.**
- **Consolidated registration, CIRMP and annual reporting for corporate groups where governance and controls are shared.**
- **Recognition of existing audits, exercises, certifications, security plans and personnel checks.**
- **A common supplier-assurance questionnaire, standard contractual clauses and recognised certification schemes.**
- **Safe harbours where entities have made reasonable efforts but cannot obtain terms or evidence from an overseas, proprietary or sole-source supplier.**
- **Worked examples for above-rail, below-rail, terminals, ports, airports, road operations, distribution facilities and digital platforms.**
- **An enforcement policy that separates serious security failure from administrative error, reasonable interpretation and good-faith remediation.**

5. Final impact analysis

Because the Rules will determine the practical regulatory perimeter, the Department cannot complete a credible final Impact Analysis until it releases exposure drafts of the Rules for comment.

The Department has identified the main cost categories but has not yet quantified them. At a minimum, the final assessment must include:

- **legal and technical advice to interpret thresholds, exclusions, asset boundaries and control tests.**
- **asset, facility, system, dataflow, supplier and interdependency mapping.**
- **registration, change notification, record keeping and annual reporting.**
- **CIRMP design, governance, maintenance, review and evidence management.**
- **independent assurance, including preparation, fieldwork, travel, multidisciplinary specialists, reporting and remediation.**
- **technology and physical-security uplift required solely by the new obligation, including work on legacy operational technology.**
- **contract review, negotiation, supplier assurance, certification review and exception management.**
- **critical-worker role mapping, background checking, access-control changes, training and workforce administration.**
- **duplicate reporting, audits and exercises where equivalence has not been resolved.**
- **management and board time, including time spent obtaining external legal and assurance advice; and**
- **transitional costs created by short commencement periods, unavailable assurance providers or delayed government guidance.**

The analysis should also:

- **identify the expected regulated population and explain which assets and entities are excluded.**
- **separate entities regulated under SOCI from newly captured entities.**
- **separate SOCI costs from enhanced CIRMP and Systems of National Significance costs.**
- **disaggregate road, freight rail, ports and maritime, airports and air freight, intermodal terminals, distribution and digital freight systems.**
- **distinguish large national, medium, regional and specialised operators, including single-jurisdiction and multi-jurisdiction businesses.**
- **publish one-off and recurring unit costs, staff-hour assumptions, professional-service assumptions and the aggregate average annual cost over 10 years.**
- **identify which existing transport-security, safety, cyber and corporate controls are treated as business as usual and explain the evidence for that assumption.**
- **count an exemption or deemed compliance saving only where the relevant instrument will be in force at commencement.**
- **assess competition, modal neutrality, regional viability, supplier concentration and cost pass-through; and**
- **be tested with affected peak bodies and operators before the Rules are finalised.**

No new freight class should be covered by the SOCI regime before this work is finished - proportionality cannot be judged otherwise.

If Parliament creates a broad freight class before the Rules and guidance are settled, industry will carry both the uncertainty and the cost.[25]

Recommended sequence

The following sequence should be followed to develop a suitable final impact analysis:

1. **Settle the Act-level architecture and release exposure drafts of the Rules, thresholds and exclusions.**
2. **Complete a sector-by-sector equivalence map and publish the proposed class exemptions and deemed-compliance arrangements.**
3. **Publish the freight-specific regulatory burden estimate, together with the broader competition and market analysis.**
4. **Release asset-boundary guidance, worked examples, designation procedures, protected-information arrangements, reporting forms, assurance standards and the enforcement policy.**
5. **After all instruments and guidance are final, allow at least six months for threshold assessment and registration.**
6. **Allow newly captured entities at least 18 months to establish and implement a CIRMP, with more time where substantial technology, infrastructure, workforce or contract changes are required.**
7. **Do not require the first independent assurance review within 24 months of CIRMP implementation unless an identified risk justifies an earlier review.**
8. **Impose enhanced CIRMP or Systems of National Significance obligations only after a separate assessment, notice and decision.**
9. **Review the freight perimeter, actual compliance cost, competition effects and security outcomes after three years, comparing the Impact Analysis estimates with costs reported by regulated entities.**

25 Department of Home Affairs, Streamlining and Modernising the Security of Critical Infrastructure Act 2018: Consultation Paper (July 2026).

6. Considerations when developing rules

Capture model

The Rules need clear criteria for each freight asset class. Where practical, they should also identify the facilities or systems covered, so government and industry know exactly who is in scope.

Before designating an asset, the decision-maker should ask five practical questions: what would the national consequences be, how quickly would they arise, what alternatives exist, how long would recovery take and what obligations already apply?

The Rules should consider:

- **how quickly disruption would affect essential goods, fuel, medicines, water-treatment inputs, emergency response, Defence movements, major trade gateways or remote communities.**
- **the number and geographic spread of affected people, communities, jurisdictions and critical infrastructure sectors.**
- **market concentration and any single or common point of failure.**
- **the capacity and mobilisation time of another route, mode, terminal, facility, system or provider.**
- **the likely duration of disruption and the time needed to restore or safely reconfigure the function.**
- **privileged digital or operational control over multiple nationally significant supply chains; and**
- **any Defence or national security role identified by the government.**

Example: *A high-throughput facility with several practical substitutes may pose less national risk than a lower-volume facility serving an isolated region with no alternate route.*

Freight services asset boundary

ALC supports the proposed focus on systems, facilities, and operational capabilities owned, operated or controlled by the freight business.

The Act or Rules should also make clear that using, accessing or depending on another asset does not amount to controlling it.[26]

A freight entity can identify its material dependencies, maintain reasonable contingencies and cooperate with the party controlling the asset. It should not be required to audit another SOCI entity, certify a State-owned corridor or reproduce controls already imposed under another asset class

Example: *an above-rail operator can manage rolling stock, crews, and disruption plans, but not assure signalling run by the infrastructure manager; a stevedore can secure its terminal but not guarantee the electricity network serving the precinct.*

Defence and national security dependencies

Defence and national security consequences belong in the criticality test; industry may have no visibility into them. A freight business may not know that a terminal, corridor, digital platform or specialist capability forms part of classified mobilisation or sustainment planning.

26 Department of Home Affairs, Streamlining and Modernising the Security of Critical Infrastructure Act 2018: Consultation Paper (July 2026).

When a dependency determines capture, the government needs to identify it through designation, protected notification, a contract, or another documented assessment.

Predominantly export supply chains

Scale and value are unreliable measures of criticality for predominantly export-dedicated supply chains. A large bulk export task can be economically significant without being essential to domestic supply, Defence or the continuing operation of another Australian critical infrastructure sector.

The Rules should exclude predominantly export-dedicated chains unless the government can show an Australian consequence: a material Defence or national security role, a domestic fuel or essential-supply dependency, reliance by another critical infrastructure sector, or disruption capable of threatening national economic stability rather than normal commercial performance.

Where only part of an asset is required for the domestic consequence, the regulation needs to be centred on risk management at the level needed to provide what is critical to the national security, domestic fuel, or essential supply objective, rather than the entire asset. For instance, if 5% of the asset use is for a SOCI-related purpose, the entity's plan should have the flexibility to focus on how it can facilitate the 5% to a SOCI standard, rather than managing the remaining 95% to the SOCI standard.

7. Responses to specific measures

Measure 13 – Critical freight

The most important measure for our industry in the discussion paper concerns the management of critical freight.

The ALC believes the justification for updating the framework is clear; however, the boundaries and definitions are not.

The current freight framework is narrow and does not consistently capture Australia's current supply chain dependencies.

Nationally significant intermodal interfaces, distribution nodes, cold-chain facilities, logistics platforms, and discrete chokepoints may fall outside existing definitions even when failure would affect more than one operator or jurisdiction.[27] [28]

Assessment of the preliminary impact analysis

The preliminary impact analysis on page 62 is directionally plausible. It correctly identifies threshold assessment, asset and systems mapping, registration, regulatory alignment and ongoing CIRMP and reporting as material cost drivers. It also reasonably recognises that multi-jurisdictional networks, specialised nodes and some regional operators may face disproportionate mapping and alignment costs.

However, the analysis does not yet provide a sound basis for concluding that competition effects will be limited. The Department has not estimated the number of entities or assets that would be captured, separated existing SOCI entities from newly regulated entities, or modelled the effect of different Rules-level thresholds. The practical outcome could range from a small number of prescribed national nodes to broad self-assessment across hundreds of facilities, systems, contracts and corporate entities.

The assessment also understates the likely cost base. It does not quantify legal and technical advice, independent assurance, operational-technology uplift, contract renegotiation, supplier assurance, critical-worker administration, board and management time, duplicate State and Commonwealth reporting, or the limited supply of suitably qualified assurance specialists. These costs will not fall evenly. Fixed compliance costs can be proportionately higher for medium, regional and specialist operators and may be passed through to freight customers, suppliers and households.

The competition risk, therefore, depends on more than the final threshold. The Department must also test whether the reforms favour large vertically integrated operators, cause smaller suppliers to exit or consolidate, distort competition between road and freight rail, or reduce regional service capacity. It should count savings from exemptions or deemed compliance only where the relevant instrument will be in force when the obligations commence.

Before Measure 13 proceeds, Home Affairs should publish a freight-specific final Impact Analysis that tests narrow, moderate and broad capture scenarios, including any connected transport systems pathway. For each scenario, it should identify the regulated population and exclusions; quantify one-off and recurring costs over 10 years; separate baseline SOCI, enhanced CIRMP and Systems of National Significance costs; and assess competition, modal neutrality, regional viability, supplier capacity, and cost pass-through with affected operators and peak bodies.

27 Department of Home Affairs, Streamlining and Modernising the Security of Critical Infrastructure Act 2018: Consultation Paper (July 2026).

28 Security of Critical Infrastructure (Definitions) Rules (LIN 21/039) 2021 (Cth), current compilation.

In relation to specific consultation questions posed in relation to the measure:

Question 62 – Is the proposed Act-level model workable?

No. The proposed Act-level model is not workable for the freight industry in its current form. The Department should not leave entities to determine the legal boundary through broad self-assessment. The Rules must clearly identify the relevant asset classes, thresholds, exclusions, and worked examples to produce consistent outcomes and avoid unnecessary legal and technical costs.

Question 63 – What criteria should distinguish nationally significant freight dependencies?

Criticality should turn on four questions: how serious the consequences would be, how quickly they would arise, what alternatives could be mobilised, and how long recovery would take.

Capture should require a demonstrated effect on essential or time-sensitive supply, on dependent critical infrastructure sectors, on major communities, on Defence or national security, and on an inability to substitute capacity before serious consequences arise. Regional assets may meet that test despite modest commercial scale, where isolation, a single route or limited storage leaves no practical alternative.

Question 64 – Does the proposed freight-services asset boundary work?

Focusing on systems, facilities and capabilities controlled by the freight business is sensible. The legislation must also make clear that using or depending on public infrastructure does not transfer responsibility for that infrastructure.

Question 65 – Should connected transport systems be capable of capture?

Yes, but only at a nationally significant scale. Capture may be justified where compromise or loss of the system would have serious consequences for transport safety, freight continuity, Defence, national security or another critical infrastructure sector. A distinct critical transport systems pathway is preferable because these systems commonly serve passenger, emergency and freight movements together.

Local roads, ordinary traffic signals, individual vehicles, small telematics systems and general-purpose public infrastructure should remain excluded. Many significant transport systems are owned or operated by States and Territories. Thresholds, reporting, incident coordination and regulatory responsibility should therefore be settled through an intergovernmental process before commencement.

Comments in relation to other selected measures proposed in the discussion paper include:

Measure 1 – Consolidated exemptions and regulatory equivalence

Home Affairs should settle the exemptions framework and proposed exemptions before new freight duties begin. At present, the interaction between SOCI and transport regulation can require businesses either to duplicate controls or seek broad exemptions that do not reflect the actual overlap.[29] Without exemptions being defined upfront before regulation commences, entities will need to go down a dual-track of applying for an exemption and implementing a CIRMP if the proposed exemption is not approved.

Equivalence needs to be assessed obligation by obligation and, where useful, hazard by hazard. Aviation or maritime law may already provide equivalent personnel security and access controls without covering every

29 Department of Home Affairs, Streamlining and Modernising the Security of Critical Infrastructure Act 2018: Consultation Paper (July 2026).

SOCI supply chain or natural-hazard requirement. Relief should apply to the equivalent part, leaving the balance of the SOCI duty intact.

Class and cohort exemptions are needed alongside individual applications. Home Affairs should publish the recognised regime, the SOCI obligations covered, any conditions, commencement and review arrangements. Where Commonwealth laws overlap, the government should resolve the interaction centrally rather than require each entity to fund its own legal case.

Measures 2 and 3 – Registration and annual reporting

ALC supports simpler registration and annual reporting. The Register should collect what the government needs for national visibility, contact and intervention, not operational details already held under transport regulation. Corporate groups operating several assets under common governance and a shared CIRMP should be able to report once, while retaining asset-level information where it is relevant.

Forms and data definitions need to be stable and available well before the reporting period. Notifications should be limited to changes that materially affect ownership, operational control, criticality or government response. The Single Reporting Portal helps entities identify their obligations, but it has not yet removed the need to complete several statutory reports.[30]

Measure 5 – Cyber incidents involving automated systems and artificial intelligence

The Act can confirm that compromise, manipulation or loss of control involving an authorised automated or AI-enabled system may amount to a cybersecurity incident when the existing thresholds are met. It should not create a separate reporting category for ordinary model error, poor output, software defects or commercial outages. Those events belong in SOCI only when a cyber event materially affects the critical infrastructure asset.[31]

Measure 6 – Systems of National Significance

ALC supports simpler Systems of National Significance obligations and recognition of equivalent exercises and vulnerability assessments. Designation is still a serious step. Objective criteria, notice, an opportunity to respond, and suitable review arrangements should remain subject to the sensitivity of the information.

A freight asset entering the baseline regime should not automatically become a System of National Significance or face enhanced CIRMP requirements. Expanding the freight perimeter and imposing enhanced obligations are separate decisions and need separate evidence.

Measure 15 – CIRMP governance and assurance

Senior accountability is appropriate, but the governing body should not be required to approve, review, update or vary a CIRMP.

This matters in large transport networks, where site arrangements, system configurations, suppliers and operating procedures change regularly. Requiring board approval for each material operational change could delay remediation and blur the line between governance and management. Proper consultation and consideration should be taken with any proposed obligations on Boards (or governing bodies) to ensure they do

30 Australian Signals Directorate, Single Reporting Portal.

31 Department of Home Affairs, Streamlining and Modernising the Security of Critical Infrastructure Act 2018: Consultation Paper (July 2026).

not impede the three lines of defence governance model or otherwise compromise the role of independent assurance. As drafted, the proposed reforms overstep.

A 24-month review cycle is a reasonable backstop if event-based reviews are limited to material changes. The law should distinguish between a review of whether the CIRMP remains current and the formal re-approval of the entire document. Mature entities should be able to rely on continuous risk and change-control processes.

Independent assurance should test design, implementation and effectiveness. A three-year base cycle, with independent internal assurance for lower-risk entities and stronger independence where risk warrants, is a workable starting point. Members nevertheless expect external assurance to be costly and largely unrecoverable. Existing work under ISO 27001, the Essential Eight, the NIST Cybersecurity Framework, accredited internal audit programs and transport security programs should be recognised. SOCI assurance should concentrate on gaps and integration rather than commissioning another full audit.[323334]

The assurance model also needs the right expertise. Few reviewers will have deep capability across cybersecurity, physical security, personnel risk, natural hazards, supply chains, and complex transport operations. A credible engagement may require a coordinated team of specialists. The Rules should allow that approach and recognise the limited provider market, particularly for regional operations and operational technology.

The cost of periodic assurance will be high, particularly when an engagement requires specialists across cybersecurity, operational technology, physical security, personnel risk, natural hazards, and complex transport operations. The Rules should define the base cycle. ALC does not support annual or 24-month independent assurance as the default. A three-year base cycle is a more workable starting point, with earlier assurance only where the asset's risk profile, a material incident or a significant control change justifies it.

ALC does not support removing all protections from annual compliance and assurance reports or treating those reports as a routine source of enforcement evidence. Mandatory assurance works only when entities can identify weaknesses candidly, explain context and prioritise remediation. If each disclosed deficiency can immediately support a civil penalty, boards, management and assurance providers will qualify reports, narrow testing and involve legal advisers at every stage. That will reduce the regulator's visibility of genuine risk, delay remediation and make assurance more expensive. Reports may also contain sensitive security architecture, vulnerabilities, supplier information and remediation plans that require strict handling and use limitations.

The CISC should use assurance reports to supervise risk reduction, target engagement and verify remediation. It should rely on them for enforcement only where a report is knowingly or recklessly false or misleading, deliberately conceals serious non-compliance, or shows serious and repeated failure to remediate after reasonable opportunities to act. Good-faith disclosure followed by prompt remediation and cooperation should remain protected unless the regulator has independent evidence of a contravention.

Reports should be available for enforcement only where they are knowingly or recklessly false or misleading, deliberately conceal serious non-compliance, or show serious and repeated failure after reasonable

32 Department of Home Affairs, Streamlining and Modernising the Security of Critical Infrastructure Act 2018: Consultation Paper (July 2026).

33 Security of Critical Infrastructure (Critical Infrastructure Risk Management Program) Rules (LIN 23/006) 2023 (Cth), compilation no. 2, 10 June 2026.

34 Security of Critical Infrastructure Legislation Amendment (Enhanced Critical Infrastructure Risk Management Program) Rules 2026 (Cth).

opportunities to remediate. A good-faith disclosure, followed by prompt remediation and cooperation, should retain protection unless the regulator has independent evidence of a contravention.

Measure 16 – Graduated civil penalties

Penalty settings need to match both the duty and the conduct. Any increase should follow, not precede, clarity on the asset boundary, Rules, assurance standards and transition. Higher penalties, while key requirements remain in future instruments or guidance, would increase legal risk without improving security.

Administrative mistakes, reasonable disputes about interpretation, late updates with no security consequences, and deficiencies identified and corrected through an assurance call warrant a lower-level response.

Measures 17 and 18 – Relevant operators and connected entities

The relevant operator concept is workable if both elements remain: material practical authority and material operational dependency. Contract value, commercial importance or the provider's label is not enough. The provider must have real authority to operate, configure, disable, restore or materially alter a critical function, and the responsible entity must materially depend on that authority.

Direct duties should cover cooperation, timely notification and conduct within the provider's knowledge and control. Registration as a relevant operator should not make the provider responsible for the broader SOCI duties of the responsible entity.

The proposed safe harbour for reasonable but unsuccessful efforts to secure contractual cooperation is important, particularly for overseas, proprietary and sole-source vendors. It should also cover contracts that cannot reasonably be changed until renewal, provided the responsible entity records the constraint and applies available alternative controls.

A cooperation duty for connected entities is also reasonable where a related company controls a system, service or information needed for compliance. The duty requires qualifications in reasonableness, capability, confidentiality, legal privilege, foreign law, data localisation, and other regulatory constraints. It should not turn every parent, subsidiary or shared-service company into a responsible entity.

Corporate groups should be able to use common governance, CIRMP, assurance and reporting where risks and controls are genuinely shared. The same group-level system should not be registered and reported repeatedly for each asset entity.

Measure 19 – Cyber assurance of major suppliers

There is a case for clearer supplier-assurance requirements.

Supplier assurance must be based on actual risk. Access, operational role, market concentration and the possible effect on the asset are more relevant than contract value or supplier size.

The Rules should recognise credible certification and accreditation, permit documented exceptions when terms or evidence cannot reasonably be obtained, and apply new contractual expectations at entry, renewal, or upon a material variation. The government can reduce duplication by developing standard clauses, a common supplier questionnaire, and clear recognition criteria. Without that coordination, suppliers will face different demands from every regulated customer, with the cost passed back through the chain and little security gain.

Measure 20 – Specified risk information

ALC supports a procedural duty to consider specified, authoritative risk information and record a reasoned response. That duty must not allow guidance, intelligence or preferred control to become a binding technical standard without proper rulemaking.

The Secretary should specify only current, relevant material and identify the affected asset classes, the commencement date, the response period, the review date, and whether an earlier item is replaced. Classified or restricted material must be delivered through channels that entities can use. An entity should remain free to adopt a different control where its documented assessment shows that it is more suitable.

Measure 21 – Critical workers and components

An access- and authority-based definition is clearer than the present circular consequence test. It should focus on people who can materially affect security or resilience through privileged system access, unescorted access to sensitive areas, access to configuration or vulnerability information, or authority over a critical function.

Operational importance alone must not bring the general freight workforce into scope. Drivers, train crew, warehouse workers and frontline operators are essential to daily service, but that is a different question. Capture should require access or authority capable of materially compromising, disabling, reconfiguring or defeating a security-critical function or component.

Controls should reflect the level of access. Privileged remote access to a national control system presents a different risk from supervised physical access. Existing ASIC, MSIC, rail, licensing, security and employment checks should be recognised as current and relevant. Transition arrangements should preserve valid clearances and avoid unnecessary re-screening.[35][36][37]

35 Department of Home Affairs, Streamlining and Modernising the Security of Critical Infrastructure Act 2018: Consultation Paper (July 2026).

36 Aviation Transport Security Act 2004 (Cth), compilation no. 39, 27 March 2026.

37 Maritime Transport and Offshore Facilities Security Act 2003 (Cth), compilation no. 31, 27 March 2026.

8. Conclusion

The current freight provisions no longer reflect the systems and interfaces on which modern supply chains depend. Some nationally significant nodes, platforms and capabilities may sit outside the Act, but the answer is not to regulate ordinary freight activity.

ALC members support stronger security. They do not support a perimeter that captures ordinary freight activity, shifts responsibility beyond an entity's control or duplicates mature transport regulation.

Success should be judged by whether the law closes a genuine national vulnerability and improves the management of that risk. A perimeter drawn too widely will instead consume scarce cyber, assurance and operational expertise through legal interpretation, duplicate audits and supplier administration.

Until that work is complete, it is not possible to determine whether the proposed regime will be effective, practical or proportionate. This work will require genuine engagement with industry participants and cross-government coordination. Industry's expectation is that there will be further significant discussion and consultation prior to any exposure drafts of legislation.

ALC is available to work with Home Affairs, transport agencies, security regulators, and State and Territory governments on detailed thresholds, exclusions, equivalence arrangements, cost assessment, and implementation guidance.

Australian Logistics Council

July 2026