Proposed Amendments to the Critical Infrastructure Risk Management Program Rules for High-Risk Asset Classes

A Submission to the Australian Department of Home Affairs

Friday,13th February 2026

Table of Contents

1. Introduction

The Australian Logistics Council (ALC) welcomes the opportunity to comment on the proposed enhancements to the Critical Infrastructure Risk Management Program (CIRMP) Rules. ALC represents the end-to-end supply chain sector in Australia, encompassing ports, stevedores, intermodal terminals, freight rail operators and infrastructure managers, airports and air-freight precincts, national warehousing and logistics property groups, major road freight and 3PL providers, and the digital platforms that support the movement and storage of freight across the country.

The national freight task depends on operational environments characterised by shared access, distributed control, and tightly coupled integrated operational technology (OT)–information technology (IT) systems. Freight and logistics assets—ports, warehouses, terminals, rail yards, airport precincts—operate with multiple entities on site at any given time, including tenants, contractors/subcontractors, labour-hire workforces, drivers, ground handlers and technology vendors. These environments are supported by complex supplier and technology networks and are under increasing pressure due to national cyber workforce constraints and OT-specialist shortages. Demand for cyber roles is rising materially faster than the broader labour market[1].

Freight and logistics infrastructure is characterised by long-lived, capital-intensive assets, many of which operate for 20 years or more. Operators face a structural tension between traditional commercial drivers—including return on shareholder equity, fiduciary duties, and regulatory obligations—and national security requirements, which are increasingly volatile and demand rapid adaptation. This tension is particularly acute in regulated segments, such as freight rail and ports, where economic constraints limit the ability to fund remediation, cyber uplift, or structural changes without government or vendor support. ALC encourages the Department to clarify how it intends to consult on the allocation of responsibility for funding critical infrastructure risk mitigation and structural change.

ALC supports uplift in critical infrastructure security. However, effectiveness will depend on proportional, risk-informed measures aligned with existing safety, operational, and regulatory frameworks. Freight operators are committed to strengthening resilience, but they manage capital-intensive assets across heavily regulated, interdependent, and workforce-constrained environments. The proposed reforms would require organisations to employ additional staff to either re-document material already captured under existing frameworks or undertake further uplift activities, imposing additional costs that are often unrecoverable from customers.

The following submission addresses each proposed enhancement individually, assessing operational feasibility, interaction with existing regulatory systems, and broader impacts on resilience, continuity, and safety across Australia's freight network.

2. Enhancement 1 – Specified Risk Advice and All-Hazards Directions

ALC supports the principle that operators should consider credible, intelligence-informed advice in managing risk. Freight operators already work with multiple streams of government advice—including Australian Cyber Security Centre (ACSC) advisories, Critical Infrastructure Security Centre (CISC) guidance, state transport alerts, emergency management notifications, and regulatory communications from bodies such as Office of the National Rail Safety Regulator (ONRSR) and the Office of Transport Security.

The operational concern is not access to advice but the administrative duplication that arises when multiple regulators require similar risk considerations to be documented separately or in prescribed formats. Freight operators already manage obligations under rail safety, aviation, and maritime security, WHS, Security of Critical Infrastructure (SOCI) and emergency management frameworks. If "specified risk advice" is defined broadly or applied retrospectively, operators may need to demonstrate—under several regimes—that identical information has been considered through multiple documentation pathways. This is inefficient for operators and undermines the intended uplift in substantive risk management.

Case study 1 – Regulatory Overlap

The Rail Safety National Law (Queensland) (RSNL) and the Rail Safety National Law National Regulations 2012 (Qld) (RSNL Regs) require rail transport operators to take a comprehensive approach to managing safety risks. Similarly, to the SOCI Act regulatory framework, these obligations cover the full range of risks that may affect safe rail operations, including risks and incidents arising from physical hazards and cyber security.

In particular, under the RSNL framework, rail transport operators must maintain a Safety Management System. This system must identify and assess safety risks, put in place controls to manage those risks, and include processes for ongoing monitoring, review, improvement, and reporting. The Safety Management System must also include a Security Management Plan. This plan must address threats to people such as sabotage, terrorism, and other security-related harms, which would include those that could be caused or enabled by cyber activity. In addition, cyber incidents that may directly affect the safe operation of railway assets are formally recognised within the national rail safety framework. These incidents are classified as Category A notifiable occurrences, meaning operators must report them to ONRSR.

ALC members also emphasised the risk created by retrospective designation of advice. If guidance originally issued as general information is later classified as "specified," operators may be required to demonstrate historical decision-making that is difficult to reconstruct, particularly for long-lived assets or geographically dispersed operations with lean risk functions.

[1] https://www.jobsandskills.gov.au/news/cyber-security-skills-demand-labour-market-evolves

ALC recommends that consideration of specified risk advice should be evidenced through existing enterprise risk and safety management systems, rather than through a parallel CIRMP documentation layer. Clear, prospective criteria for what constitutes “specified risk advice” would ensure obligations are workable, targeted, and focused on genuine uplift rather than recordkeeping duplication.

3. Enhancement 2 – Uplift to Cyber Maturity Level 2 (or Equivalent)

ALC supports uplift to a stronger cyber maturity baseline. The ACSC Annual Cyber Threat Report 2024–25 identifies critical infrastructure as the most frequently targeted sector for major cyber incidents[2]. Freight and logistics operators continue to experience increasing threat activity consistent with international trends targeting transport and supply chains. However, the feasibility, timing, and cost of uplift vary significantly across modes.

- **Ports and stevedores** rely on OT systems—cranes, yard equipment, TOS platforms—that are vendor-controlled and require coordinated engineering outages aligned with shipping schedules.
- **Air-freight precincts** depend on aviation security systems and time-critical freight screening: identity and access uplift must not introduce latency in flows essential to just-in-time supply chains.
- **Warehouses and national logistics property** rely on large-scale automation platforms (autonomous mobile robots (AMRs); AMRs, conveyors, warehouse management and control systems (WMS/WCS), building management systems (BMS)). Cyber uplift is dependent on secure integration, segmentation, vendor remote-access controls and logging—not simply policy compliance.
- **Road freight and 3PL operators** face uplift challenges across dispersed subcontractor fleets reliant on mobile devices and shared cloud platforms.
- **Rail and intermodal operators** must align uplift with RSNL change management processes, consultation expectations and existing safety assurance requirements. Legacy OT assets with long renewal cycles and extended operational lifespans limit the pace of uplift, creating tension between commercial viability and security obligations. The industry-supported National Transport Commission’s (NTC) National Network for Interoperability reforms may create additional tension with the potential for higher reliance on certain vendors.

In the absence of government-mandated cyber security standards for technology vendors supplying critical infrastructure (and including what reliance can be placed on SOCI-regulated Data Storage or Processing entities), the proposed reforms will result in individual operators bearing the full cost of cyber security uplift in the products they use. This places the economic burden entirely on operators, rather than vendors better positioned to implement improvements.

Case study 2 – Member Funding Cyber Uplift for Products from Multiple Vendors

Manufacturers are rapidly advancing and deploying OT technology solutions for safety, diagnostic data collection, connectivity, and data integration. However, the rush to be first to market has resulted in many solutions lacking adequate cyber security considerations. The challenges of interconnectivity and compatibility often leave operators with limited options when acquiring these technologies.

Recently, a member collaborated with three different locomotive product manufacturers over a two-year period to enhance their cyber security awareness, improve software development practices, and implement controls such as authentication, secure file transfer, and physical port restrictions. This industry-benefitting involvement was funded entirely by the member who operates the relevant products.

A binding constraint across all modes is workforce capacity. National cyber workforce shortages are well documented. Demand for cyber roles is outpacing supply, with OT-capable security engineers particularly scarce[3]. Industry analysis indicates Australia may face a shortfall of up to 30,000 cyber specialists by 2030 if current trends persist[4]. The proposed uplift will place further pressure on this already over-extended skillset, resulting in higher costs to operators. Freight operators have limited ability to recover these costs from customers compared with other sectors subject to enhanced CIRMP obligations.

ALC recommends targeted support to develop mid-career and senior engineering cyber talent, where the gap is most acute. Industry supports a staged, risk-based approach to maturity uplift aligned with capital cycles, vendor availability,

[2] https://www.cyber.gov.au/resources-business-and-government/government/annual-cyber-threat-report-2024-25

[3] https://www.jobsandskills.gov.au/publications/occupational-shortages-list

[4] https://cybercx.com.au/news/cyber-skills-shortage-to-hit-30000-in-four-years/

and workforce capability. Recognition of functional equivalence allows operators to achieve Level 2 outcomes through different architectures. Prioritising ACSC high-value controls—comprehensive logging, secure remote access, and legacy mitigation—will produce the strongest uplift under current workforce constraints. Government incentives, such as a tax offset for cyber security investment, could help defray costs, analogous to the Research and Development tax incentive model.

Members emphasised that, cumulatively, the proposed technical requirements risk shifting the cyber posture of freight operators from that of a commercial infrastructure operator to that of a high-risk government or defence provider. Achieving and maintaining this level of maturity would require substantial and ongoing capital and operational expenditure, including specialist engineering redesign, vendor re-architecture, additional monitoring capability, continuous assurance activities, and sustained workforce uplift. In a capital-intensive, margin-constrained sector operating high-value, long-term assets, such expenditure would necessarily be diverted from other operational risk controls, safety investments, resilience upgrades, or decarbonisation priorities. A prescriptive uplift model may therefore produce unintended consequences, whereby organisations prioritise compliance with a single regulatory framework over broader enterprise risk management activities informed by their own threat assessments. In some cases, this could reduce overall organisational resilience rather than strengthen it.

ALC submits that maturity expectations must be calibrated to reflect the risk profile of freight infrastructure and should remain grounded in the “so far as is reasonably practicable” standard embedded in the SOCI framework. Government should clarify whether the intent is equivalence with commercial best practice or alignment with national security-level assurance models, as the cost and structural implications differ materially.

4. Enhancement 3 – Critical Systems Network Segregation

ALC supports network segregation as an important cyber security objective. However, freight operations depend on elevated levels of interconnectivity between OT and IT systems.

Real-time yard coordination in ports, robotics in warehouses, rail network scheduling, telematics platforms and airport freight systems all rely on continuous data exchange. Prolonged isolation of critical systems would introduce operational risks—including the need for manual reversion of equipment, misaligned scheduling, interruptions to yard and gate coordination, and delays in processing freight held within controlled zones.

Case study 3 – Interconnectivity

The operation of containerised freight on rail relies heavily on the seamless interaction of multiple systems to fulfill health and safety obligations under RSNL, state based WHS laws/regulations, including Dangerous Goods and Major Hazardous Facilities requirements. For instance, a freight forwarder books a container of Dangerous Goods through an internet interface into a freight booking system. This system then interfaces with the Terminal Operating System (TOS), to enable delivery or storage within licenced DG limitation (noting levels may be different depending on type of chemical, state of departure/arrival, site/operator licences).

Next, the TOS interfaces with a rail consist planning system to enable the train design, safe segregation of DG, and adherence to on-train limits for the train operator. The rail consist, including details of the DGs being carried, is sent via IT systems to the relevant below-rail network providers, who use this information to operate safely, involving both IT and OT components. These manifests are then printed and accompany the train to support emergency services respond to an emergency, if required.

Finally, the receiving terminal's TOS must communicate the train’s arrival and container information, including DG information. Generally, the trucking operator, who will likely differ from the freight forwarder, makes truck bookings to deliver or pick up containers at terminals through a web interface.

If full segregation of system components were required, numerous manual interventions would need to replace automated, control-rich processes. While this may reduce certain cyber exposure pathways, it would materially elevate other risks that must also be managed to a SFAIRP standard.

The consultation paper’s expectation that critical systems demonstrate operational independence for up to three months while maintaining critical services presents significant feasibility challenges in this context.

Freight systems are not stand-alone assets. They operate as interdependent chains of interaction across multiple organisations. Enterprise systems in large retail and distribution networks exchange data tens of thousands of times daily with supplier systems, transport providers, terminal operators, and freight forwarders to enable purchasing, consignment creation, inventory control and dispatch. Prolonged digital isolation would remove the real-time data necessary to operate safely, lawfully, and efficiently. Replicating this volume and complexity through manual business continuity arrangements would not be operationally realistic.

Extended isolation would also increase material operational and safety risks, including:

- breakdown of dangerous goods tracking and manifest integrity;
- loss of fatigue and safe-working system synchronisation;
- scheduling conflicts across freight rail and port interfaces;
- congestion and queuing at terminal gates;
- disruption to just-in-time supply chains for essential goods.

ALC submits that the appropriate objective is rapid containment and controlled system reconstitution, rather than sustained disconnection from integrated supply chain ecosystems. Segregation requirements should therefore focus on limiting lateral movement and enabling swift isolation of compromised components, while preserving safe-working systems and regulated scheduling processes. This is particularly critical during peak demand periods and extreme weather events. Increased frequency of severe weather[5] affecting key road and freight rail corridors underscores the need for system resilience and rapid recovery capability rather than prolonged operational separation.

5. Enhancement 4 – Multi-Factor Authentication (MFA)

MFA is a high value control that ALC supports, particularly for privileged and remote access. Operational environments in freight, however, present practical constraints that must be recognised.

Drivers, subcontractors, and labour-hire workers often connect via personal mobile devices. Terminals and warehouses frequently use shared workstations. Vendor remote access into legacy OT remains common. Regional rail and road operations may encounter intermittent connectivity, and many safety-critical rail and aviation tasks require uninterrupted access pathways. Given that OT systems are often long-lived assets with design lives of up to 30 years, MFA implementation is frequently not technically feasible without significant system redesign.

ALC members were clear that MFA must not impede fatigue-critical operations, emergency response, freight prioritisation during extreme weather, or safe-working systems mandated under RSNL. Authentication failures in these contexts present direct safety and continuity risks.

ALC supports multi-factor authentication (MFA) for privileged and remote access where operationally feasible. Where MFA is not practicable, compensating controls—such as hardened jump hosts, supervised access, or device-based certificates—should be acceptable. Clear government guidance on such alternatives would ensure uplift without compromising operational safety.

ALC notes that the SOCI Act establishes a risk-management obligation “so far as is reasonably practicable” (SFAIRP). The proposed enhancements risk introducing prescriptive technical measures through the Rules, which could shift the practical application of the Act from principles-based risk management to a compliance-focused, prescriptive model. ALC maintains that critical infrastructure owners are best positioned to develop controls appropriate to the unique risks of their assets, using MFA and other measures in line with SFAIRP principles, rather than being compelled to adopt uniform, mandatory technical solutions that may not be feasible across diverse operational environments.

6. Enhancement 5 – Advanced Technologies and Artificial Intelligence

Freight operators are among the largest adopters of advanced technologies and AI applications, including predictive maintenance, robotic automation, routing optimisation and operational modelling. In these settings, AI risks are predominantly operational: data integrity, model manipulation, optimisation drift, and alignment between automated processes and safety obligations.

Most freight operators rely on vendor-provided platforms rather than developing AI models in-house. As a result, compliance with AI governance frameworks such as ISO/IEC 42001 is not feasible without substantial vendor alignment. Mandating certification at this stage risks creating a standalone compliance requirement disconnected from operational risk, diverting attention away from actual technology controls.

[5] http://www.bom.gov.au/state-of-the-climate/2024

ALC supports incorporating emerging-technology risks into existing risk frameworks and encourages government to develop freight-specific AI threat scenarios. This approach promotes uplift without imposing premature or impractical certification obligations and aligns economic feasibility with security objectives.

7. Enhancement 6 – Supply Chain Mapping and Dependency Identification

Freight supply chains are exceptionally broad. A national 3PL may engage thousands of contractors/subcontractors; ports may operate through multiple tiers of integrators; warehouses depend on extensive automation and maintenance providers; and road freight relies on transient, seasonal, and subcontracted labour markets.

Mapping every supplier to the level suggested in the consultation paper would produce significant administrative burden with limited additional risk insight. Members highlighted that the most critical dependencies relate to OT system vendors, cloud and telecommunications providers, fuel supply and terminal operations, and core logistics software platforms. These are the suppliers where disruptions would have the most material impact on freight continuity, and where cost and risk constraints are most acute.

Determining whether suppliers are also critical to other critical infrastructure entities is not feasible without government intelligence. Operators have no visibility into cross-sector reliance beyond their contractual relationships.

ALC supports a tiered, risk-based approach focused on essential dependencies. Government-provided risk profiles for vendor classes of national security significance would substantially improve accuracy and reduce the economic burden on operators.

8. Enhancement 7 – Vendors of Concern and Foreign Ownership, Control, or Influence

Freight operators support stronger management of vendor risk, including foreign ownership, control, or influence considerations. Ports, rail, warehouses and 3PLs rely heavily on global vendors for automation systems, OT hardware, cloud services and logistics platforms. These dependencies cannot be eliminated but must be managed systematically.

Operators, however, cannot independently assess complex global ownership structures due to commercial confidentiality, integrator-led procurement pathways, and limited visibility into supply-chain provenance. Critical intelligence holdings necessary to identify high-risk vendors sit with government.

ALC members also raised concerns about the absence of baseline market-entry standards for OT vendors supplying critical logistics infrastructure. Without such standards, any developer capable of delivering code or equipment can operate in the OT market irrespective of security maturity, which increases systemic risk and economic exposure for operators.

ALC supports a shared-responsibility model in which government provides clear vendor-risk signalling and industry applies that guidance through procurement governance, contractual controls, and diversification strategies. National OT vendor standards or accreditation thresholds would further strengthen assurance for critical freight assets and provide clarity on who funds risk mitigation.

9. Enhancement 8 – Personnel Security and Critical Worker Identification

The personnel security enhancement, as currently drafted, presents substantial challenges for freight operators because its underlying assumptions do not reflect the operational and structural realities of freight infrastructure. As highlighted in the introduction, freight nodes—ports, intermodal terminals, warehouses, and airport precincts—are high-throughput, multi-operator environments where access is shared across operators, tenants, labour-hire workforces, transport companies, ground handlers, maintenance contractors/subcontractors, and technology vendors. In many facilities, the responsible entity directly employs only a minority of individuals requiring access on any given day.

The current drafting implicitly assumes a contained, controllable workforce and clearly defined access boundaries. Transposing this model onto freight infrastructure risks creating obligations that are operationally unachievable, economically disproportionate, and materially detrimental to asset throughput and continuity.

Existing regulatory frameworks already govern the highest-risk categories of workers:

- Aviation and maritime precincts use Aviation Security Identification Cards (ASIC) and Maritime Security Identification Cards (MSIC) for unescorted access.
- Rail operations regulate safety-critical workers under the Rail Safety National Law.

- Work Health and Safety (WHS) obligations provide robust induction, competency, fatigue management, and emergency preparedness controls.

The proposed CIRMP enhancement risks duplicating, conflicting with, or exceeding these existing frameworks. A broad “critical worker” category applied across multi-employer sites would intensify labour shortages—particularly during seasonal peaks—and introduce operational bottlenecks that could materially compromise freight throughput, economic efficiency, and national supply chain resilience. Freight and logistics infrastructure is deliberately designed for controlled but direct access to facilitate high-volume logistics operations. Attempting to impose a closed-campus security model would invert this operational logic and impose obligations that operators, landlords, and tenants cannot discharge without compromising both operational safety and economic viability.

ALC members raised substantive concerns regarding the mandating of AusCheck background checks as the primary risk mitigation mechanism.

AusCheck assessments are point-in-time criminal history checks. They do not assess behavioural or psychological risk indicators, provide continuous monitoring, or address insider threat factors such as coercion, financial distress, or malicious intent. Nor do they account for changes in personal circumstances after clearance is granted.

Further, AusCheck is restricted to onshore critical workers. Many freight operators rely on offshore third-party workforces and global technology vendors with privileged remote access to operational and technology systems. Mandating onshore background checks without addressing offshore privileged-access pathways creates an uneven control framework and may not materially reduce overall risk exposure.

ALC is not opposed to the need for a stringent approach to critical workers. However, personnel-security measures must both:

1. Practically identify elevated risk; and
2. Mitigate that risk in an evidence-based and operationally effective manner.

Absent this alignment, mandatory background checks may impose significant administrative burden and exacerbate workforce constraints while delivering limited incremental security benefit. A more proportionate and effective model would focus on roles involving elevated operational or technical privileges, rather than broad categories of site access.

ALC recommends:

1. **Focus on Privileged Access:** Define “critical worker” to include only individuals with elevated operational privileges, control-room authority, access to critical operational consoles, safety-system override capability, or responsibilities where compromise would materially affect asset integrity.
2. **Role-Based and Technical Mitigation:** Complement background screening with strict privilege limitation and segregation of duties; enhanced logging and anomaly detection for privileged access; time-bound access provisioning; contractual security controls for offshore vendors; integration of insider-threat awareness into existing safety and risk culture frameworks.
3. **Alignment with Existing Frameworks:** Integrate personnel-security obligations with aviation, maritime and rail safety regimes to avoid duplication and regulatory conflict.
4. **Shared Responsibility Model:** Clarify how obligations are distributed among landlords, operators, tenants, and contractors, recognising that no single entity has full visibility or control over the on-site workforce in multi-operator freight environments.
5. **Operational Feasibility and Scalability:** The Department should clarify how AusCheck processes will scale to accommodate a large influx of Critical Worker applications. Consideration should be given to enabling a portable Critical Infrastructure Security Identification credential to allow personnel to work across multiple critical infrastructure organisations without repeated clearance processes, thereby reducing administrative burden while maintaining operational throughput.

Finally, the drafting appears to conflate the Critical Infrastructure Asset with the Responsible Entity as a whole. For many logistics companies, a designated asset may represent only a small fraction of overall operations. Applying enhanced personnel-security measures across the entire organisation would impose disproportionate costs, reduce competitiveness, and misalign security objectives.

Personnel-security obligations should therefore apply to the designated asset and associated risk perimeter, consistent with the SOCI Act’s “so far as is reasonably practicable” standard. A targeted, risk-informed approach is essential to strengthen resilience while maintaining the efficiency and continuity of Australia’s freight networks.

10. Enhancement 9 – Physical Security Plan

ALC notes that the proposed Physical Security Plan builds on the risk-management principles outlined in Enhancements 1–8, including proportionality, shared responsibility, and recognition of existing frameworks. The sector's priority is targeted, evidence-based security for assets where compromise would materially disrupt operations or endanger public safety. This proposed reform duplicates existing regulations in the rail, maritime and aviation contexts. The proposed amendments do not clearly explain the specific regulatory gap they seek to address, nor how the proposed reforms would appropriately respond to the identified risk.

ALC supports a risk-proportionate, asset-focused approach consistent with the Protective Security Policy Framework (PSPF), with the following key principles:

- **Materiality-driven focus:** Security measures should be applied to assets whose compromise could significantly affect freight continuity or safety, including control centres, signalling systems, fuel depots, intermodal terminals, and ports. Lower-risk infrastructure should not be subject to identical treatment and any enhancements need to be focused on critical assets, not the organisation.
- **Integration with existing frameworks:** Existing obligations under the Rail Safety National Law, aviation, and maritime security legislation, WHS, and emergency management frameworks should be recognised as evidence of compliance where equivalent risk mitigation is in place.
- **Clear allocation of responsibilities**: In multi-operator environments, obligations should delineate the roles of asset owners, operators, tenants, and contractors/subcontractors to avoid gaps or duplication.
- **Operationally feasible controls:** Measures such as perimeter fencing, controlled access points, CCTV, alarms, and monitoring of critical components should be prioritised at high-risk locations and implemented in line with maintenance and asset renewal cycles, ensuring freight flows and safety are not disrupted. It is also relevant to note that workforce sensitivities remain in this area, with some unions expressing concerns about the scope and use of workforce surveillance measures, including CCTV.
- **Personnel security requirements**: Any obligations for personnel to obtain security clearances should be risk-proportionate and legally justified. Industry organisations may not be able to mandate clearances absent a government requirement, and such measures must be balanced against obligations under the Privacy Act. Security clearance requirements should therefore apply primarily to personnel working for government entities or contexts where there is a demonstrable, material risk to operations or public safety, rather than as a blanket expectation across the freight sector.
- **Consolidation rather than duplication:** The Physical Security Plan should integrate existing safety, security, and emergency arrangements, avoiding parallel reporting requirements or unnecessary capital expenditure.

ALC recommends that the Department workshop with Industry and then publish freight-specific guidance, including worked examples for linear infrastructure, intermodal terminals, warehouses, and ports. This would ensure consistent uplift, practical implementation across multi-operator environments, and alignment with operational realities across Australia's freight system.

11. Conclusion

The end-to-end supply chain sector supports uplift in critical infrastructure security. Freight and logistics infrastructure is essential to Australia's economic performance and increasingly exposed to sophisticated threats. Government and industry share responsibility to ensure that enhancements to the CIRMP Rules are proportionate, implementable, and compatible with real-world logistics operations. Across multiple enhancements, members have raised concerns that the cumulative effect of the proposed Rules could shift the regulatory posture from principles-based risk management toward a prescriptive national-security model, more appropriate for high-classification government environments. Freight infrastructure is critical but operates within commercial, multi-operator ecosystems. Effective uplift will require shared responsibility with technology vendors and integration with existing safety, operational risk, and regulatory frameworks.

This submission provides a cross-modal assessment of each proposed enhancement, grounded in operational experience and supported by evidence. ALC remains committed to working with the Department to refine implementation approaches that achieve meaningful risk reduction while maintaining the productivity, resilience, and continuity of Australia's supply chains.