PO Box 7182
Cloisters Square WA 6850
Tel: +61 8 6163 5400
atco.com.au

13 February 2026

Critical Infrastructure Strategy
Department of Home Affairs
Locked Bag 7
Northbridge WA 6865
CI.Strategy.Guidance@homeaffairs.gov.au.

Private & Confidential

To: Department of Home Affairs

Re: Security of Critical Infrastructure (Critical Infrastructure Risk Management Program) Rules Proposed Amendments

Thank you for the opportunity to provide feedback on the proposed enhancements to the Security of Critical Infrastructure (Critical Infrastructure Risk Management Program) Rules, as outlined in the consultation paper and presented at the town hall sessions held on 12 December 2025 and 27 January 2026.

ATCO supports the intent of the proposed enhancements and recognises the Department of Home Affairs ('the Department') objectives in strengthening the framework. ATCO's primary concerns relate to the proposed timelines and the level of prescription to operationalise certain requirements, which present practical challenges from a resourcing, capability, and cost perspective, particularly where significant uplift is required within compressed implementation periods. Greater flexibility through more flexible timelines and less prescriptive regulatory requirements would enable responsible entities to apply a risk-based approach that reflects the scale, complexity, and criticality of their operations. This would allow organisations to demonstrably reduce risks to so far as is reasonably practicable, while supporting proportionate, effective, and sustainable compliance with the intent of the regulatory framework.

All-Hazards Measures 1: Consideration of Specified Risk Advice

ATCO supports the requirement for responsible entities to consider government issued, intelligence-based risk advice, and agrees that formalising this obligation within the CIRMP framework is appropriate given the evolving threat environment. To avoid misinterpretation and support effective implementation, ATCO considers it necessary that any specific risk advice issued by government bodies is clearly articulated, including its intent, scope, and applicability. Greater clarity is needed on the breadth of the guidance, its application across different sectors and asset classes, and assurance that the analysis is directed by national security agencies with the capability to accurately assess and interpret threat environments.

ATCO also suggests that guidance from the Department on how the required level of assessment should be operationalised in practice, including expectations around assessment processes, decision making records, and the evidence requirements would be of great assistance to responsible entities to remove uncertainty and enable accelerated implementation. ATCO proposes that there is a need for greater flexibility regarding the proposed implementation timeframes. The review and implementation period for specific risk advice needs to have sufficient flexibility to allow for legitimate variances in timeframes depending on resourcing requirements, cost impacts, and the time needed to assess risks, update the CIRMP, and implement actions to achieve compliance.

All-Hazards Measures 2: All-Hazard Material Risks – Foreign Ownership, Control and Influence

ATCO supports the inclusion of Foreign Ownership, Control or Influence (**FOCI**) assessments within the CIRMP to strengthen supply chain resilience and business continuity. ATCO notes that implementation of these requirements may involve additional cost and resourcing considerations, and that without greater flexibility, the proposed timeframes could be challenging. In some cases, vendor diversification is constrained by specialised operational technology, proprietary solutions, and safety critical requirements. Reduction of FOCI risk in the supply chain may not be practicable, and having additional mitigation controls provides the most viable approach. ATCO would welcome the provision of guidance from the Department on assessment tools, standardised procurement questions and due diligence processes to ensure effective risk management of FOCI risk.

Cyber And Information Security Hazard Measures 1: Cyber Security Framework Uplift

[redacted]

Cyber And Information Security Hazard Measures 2: Critical Systems Network Protection

ATCO supports the intent of strengthening segregation to reduce the risk of compromise to critical systems and already applies layered network protections to separate critical Operational Technology (**OT)** system environments from corporate IT and internet facing systems.

In respect of the proposal for ensuring critical systems are operationally independent from other IT systems and networks to the greatest extent possible, such that they can be isolated for a period of 3 months while maintaining critical services, ATCO suggests that while some responsible entities may be able to achieve this within a relatively short time period, there are significant challenges including cost, resourcing and risk assessment processes that will require some flexibility in the time periods in which the necessary actions are to be taken. Having, for example, a prioritisation guideline and associated criteria would be a potential option that would provide the necessary flexibility.

ATCO would welcome a risk-based, outcomes-focused approach that recognises asset specific constraints, allows for staged uplift over time, and permits the use of alternative controls where full segregation or long-term isolation is not possible, while maintaining safety and reliability

Cyber And Information Security Hazard Measures 3: Multi-factor Authentication (MFA)

ATCO supports the proposal to require Multi-Factor Authentication (‘MFA’) for internet-facing systems, remote access, and privileged user access.

[redacted]

[redacted]

[redacted]

Cyber and Information Security Hazard Measure 4: Enhanced Cyber material risks

On the deployment of advanced and emerging technology, and use of such technology by malicious and state-sponsored actors against the asset, ATCO and other responsible entities are limited in their influence over vendors use of artificial intelligence (AI) in their products. The cost and time to move away from vendors that do not achieve baseline security must be acknowledged. Greater clarity is needed from the Department on vendor requirements to ensure that these can be built these into vendor contracts early and existing vendors consulted.

ATCO, like other responsible entities, would want to utilise Artificial Intelligence (**AI)** and gain all the benefit that comes with technology. Even though ATCO has an AI Standard providing guidance on what can be implemented and used in the organisation, this does address what cloud services vendors implement. For instance, when certain cloud services were adopted, AI was not part of their products, but now due to the competition in the market most of the vendors are adopting AI as competitive advantage. Knowing this and knowing the government direction on limiting the use of certain AI solutions/product guidance has to provide guidance as to how responsible entities can go about dealing with vendors especially existing vendor who are adopting AI. There will be occasions where critical infrastructure organisations cannot influence vendors decisions on their choice of AI partner. Where government has provided direction, the cost and time of moving away from those vendors must be considered.

Supply Chain Hazard Measures 1: Supply Chain Vulnerability Mapping

ATCO supports the implementation of supply chain vulnerability mapping and recognises its role in enhancing overall business resilience. The term vulnerability creates uncertainty about how deeply supply chain risks must be assessed, from tier-3 dependencies to supplier IT/OT, WHS, and sub-supplier resilience. While this reflects best practice, it may be impractical for some assets, and SOCI's expected depth of risk assessment remains unclear. Implementation timeframes may also need to be flexible to accommodate asset-specific recovery and restoration requirements, reflecting the unique design characteristics of individual critical infrastructure assets. A full mapping process that includes FOCI considerations and continuous reviews will require significant resources and investment, making it challenging to meet the prescribed timelines.

Supply Chain Hazard Measures 2: Vendors of Concern.

ATCO supports the requirement to assess and manage vendors of concern, including the consideration and assessment of FOCI risks. ATCO would welcome further Departmental guidance to assist with the clear and consistent identification of vendors of concern. Tracing foreign ownership risks through multitier supply chains is highly complex, raising concern over how far organisations are required to go with their due diligence processes and what will be deemed 'reasonably practicable'.

ATCO also notes the importance of maintaining a risk-based and pragmatic approach, particularly in circumstances where alternative suppliers may be limited (in some cases to a sole vendor), and where the use of a vendor remains necessary to support continuity of operations.

Personnel Security Hazard Measures 1: Personnel Security Plan

ATCO supports the proposal to establish and maintain a personnel security plan and welcomes clear, practical guidance from the Department on defining critical workers within its existing CIRMP and associated documentation.

Personnel Security Hazard Measures 2: Strengthened Background Checking

ATCO supports the requirement to identify critical workers and apply AusCheck screening to designated domestic-based roles but would request flexibility regarding the prescribed compliance timeframes. The current indicative 6-week ASIO assessment period does not align with standard onboarding timelines for critical roles and has proven challenging for many critical infrastructure owners. ATCO supports consideration of a reduced 4-week assessment timeframe to better align with workforce onboarding needs or the use of alternate background screening providers

ATCO also notes that implementing AusCheck processes requires significant planning, governance changes, and resourcing, with associated cost impacts. Greater flexibility in compliance timeframes would better reflect these practical constraints and support effective implementation. ATCO supports the use of risk-based controls for offshore personnel where AusCheck is not practicable and welcomes Departmental guidance in this area.

If you have any questions or would like to discuss any of these issues further, please don't hesitate to contact me.

Yours faithfully

Simon Byrne
General Counsel & Company Secretary
ATCO Australia