**JOINT SUBMISSION**

# Consultation on proposed amendments to the Ministerial Directions Powers in Part 3 of the Security of Critical Infrastructure Act 2018, and the Exposure Draft of the enhanced Critical Infrastructure Risk Management Program Rules

---

**Submitted to:** Cyber and Infrastructure Security Centre, Department of Home Affairs

**Closing date for submissions:** 1 May 2026

**Date of this submission:** 30 April 2026

---

**Authors**

**Michael Outram APM**

Principal, Michael Outram Advisory; Distinguished Advisor, ANU National Security College; former Commissioner of the Australian Border Force and Comptroller-General of Customs (May 2018 – November 2024).

**Michael Eales**

Partner, Subject Matter; Certified Chair and Design Advisor to the Australian Design Council.

# Executive summary

This joint submission responds to the Department of Home Affairs consultation opened on 25 March 2026 on two concurrent reforms under the Security of Critical Infrastructure Act 2018 (Cth) (the SOCI Act): proposed amendments to the Ministerial Directions Powers in Part 3, and the Exposure Draft of the enhanced Critical Infrastructure Risk Management Program (CIRMP) Rules. Both close for submissions on 1 May 2026.

We write as independent advisors with deep operational, strategic and commercial experience across Australia's border, aviation, maritime, supply chain and critical infrastructure systems. The views expressed are our own and are offered as a public expert contribution to an open consultation. Our standing, advisory relationships and declared interests are set out at Annex A.

The consultation is taking place at a moment of unusual strategic consequence. On 16 April 2026, the Government released the 2026 National Defence Strategy (NDS) and 2026 Integrated Investment Program (IIP). The NDS substantially broadens the concept of national defence to make civil preparedness, fuel security, economic security and supply chain resilience explicit and central. The IIP commits an additional $53 billion over the decade, funded in part through 'alternative financing where appropriate', and explicitly names counter-uncrewed air systems to protect Australian sites, events and critical infrastructure as a capability priority. Read with the SOCI reforms before the Department, the three announcements together signal that the perimeter of Australian national defence now runs through civilian critical infrastructure and that the regulatory, governance and co-investment architecture to match has to be built.

The reform window also coincides with an international inflection point. Australia is co-convening the WTO Joint Statement Initiative on E-Commerce with Japan and Singapore. The Australia–Singapore Digital Economy Agreement and the joint ACCEPT initiative provide a working bilateral framework for digital trade trust. The OECD Trade Facilitation Indicators provide an internationally comparable measurement framework. Multilateral standards reform — led by the International Chamber of Commerce Digital Standards Initiative (ICC-DSI), funded by the Asian Development Bank and now scaling with the World Bank, and by UN/CEFACT through the United Nations Transparency Protocol, Verifiable Trade Documents and the Global Trust Registry — is building the trust infrastructure that the next generation of trade and border systems will rely on. The SOCI reforms can and should be designed to align with that international architecture rather than as a purely domestic regulatory uplift.

Against that backdrop, our core proposition is that the SOCI Act reforms before the Department are necessary but incomplete. They strengthen the regulatory overlay on individual responsible entities and enhance ministerial powers for serious national-security risks. They do not, by themselves, build the system-level architecture required for federated visibility, trusted supplier assurance, cross-portfolio decision-making, international standards alignment and outcomes-based co-investment. In that sense, the reforms should be finalised, but paired with an implementation architecture capable of treating critical infrastructure, and the border that connects it, as a strategic national asset.

We endorse the direction of the proposed reforms, subject to targeted refinement, and recommend that they be paired with a cross-portfolio implementation architecture. Our headline recommendations are:

1. Endorse the enhanced CIRMP Rules in principle, subject to implementation timeline adjustments for high-risk asset classes, explicit recognition of the border as a connector across critical infrastructure, an all-hazards physical security requirement that includes counter-UAS risk consistent with the 2026 IIP priority, and alignment of the supply chain obligation with the international standards architecture for digital trade trust.

2. Support the five Ministerial Directions Powers measures in principle, with procedural safeguards strengthened to protect against regulatory surprise, and with the disclosure-delay power limited to clearly defined and time-bounded circumstances.

3. Align SOCI implementation with a federated National Border Visibility Platform (NBVP) and a National Border Investment Framework (NBIF) — both proposed in *Beyond the Checkpoint: Managing Australia's Border as a Strategic Economic and National Security Asset in a Multipolar World* (Outram, ANU National Security College Occasional Paper, January 2026), and developed in Part C of this submission, to provide the system-level architecture the expanded national defence concept requires.

4. Pilot a cross-portfolio regulatory sandbox spanning SOCI, customs, biosecurity, aviation and maritime; extending the Controlled Trials Act 2023 mechanism beyond its current customs scope, to test enhanced CIRMP obligations, directions powers and co-investment mechanisms at Brisbane 2032-relevant assets, with a bilateral corridor element anchored to the Australia–Singapore Digital Economy Agreement and the ACCEPT initiative, and with sandbox KPIs aligned to OECD Trade Facilitation Indicators.

5. Treat industry and institutional co-investment as a first-class outcomes-based funding mechanism for CIRMP uplift, with capital deployed against measurable capability and resilience outcomes, drawing on the IIP's 'alternative financing' language and the Advanced Strategic Capabilities Accelerator (ASCA) procurement model, and stacking with existing Commonwealth research collaboration and supply-chain resilience funding instruments.

6. Establish a standing Critical Infrastructure Co-design Council within the Cyber and Infrastructure Security Centre (CISC), with cross-portfolio membership including DFAT given the international and trade facilitation dimensions of the implementation phase, to sustain structured industry input across the implementation phase.

The remainder of this submission sets out the context, our assessment of each consultation track in turn, the cross-cutting architecture we recommend, and the mechanisms to deliver it.

# Contents

# 1. Scope of this submission and authors

## 1.1 Scope

This is a single joint submission covering both consultation tracks published by the Department of Home Affairs on 25 March 2026:

- Consultation on proposed amendments to the Ministerial Directions Powers in Part 3 of the SOCI Act (the Directions Paper).
- Exposure Draft of the enhanced Critical Infrastructure Risk Management Program Rules under the SOCI Act (the CIRMP Exposure Draft).

We recognise the Department has asked that separate submission forms be lodged for each initiative. We will submit this combined paper as the substantive evidence base, cross-referenced from each submission form, so that the interaction between the two instruments — and between them and the broader national defence, border reform and international trade facilitation agenda — is visible to decision-makers in one place.

The submission draws on: the ANU National Security College Occasional Paper ‘Beyond the Checkpoint — Managing Australia’s Border as a Strategic Economic and National Security Asset in a Multipolar World’ (January 2026); the Border Futures Forum held at the Port of Brisbane on 26 March 2026; published Commonwealth and Defence material; international standards and trade facilitation source material; peer-reviewed literature; and the authors’ own operational and industry experience. All factual claims are sourced from material in the public domain. A consolidated list of sources is at Annex B.

## 1.2 About the authors

Michael Outram APM was Commissioner of the Australian Border Force and Comptroller-General of Customs from May 2018 to November 2024. He now runs Michael Outram Advisory, is a Distinguished Advisor at the ANU National Security College and serves in declared independent advisory roles to a small number of Australian and international entities operating in the border, supply-chain and security-technology domains. His Occasional Paper for the ANU NSC, published in January 2026, sets out a system-of-systems framework for Australia’s border that the recommendations in this submission directly reflect.

Michael Eales is a Partner at Subject Matter, a Brisbane-based strategy consultancy. The firm advises the boards and leadership teams of Australia's critical infrastructure — maritime ports, airports, water and energy utilities — supply-chain identification and digital trade standards organisations, and the institutions shaping Australia's national design and innovation system. Subject Matter's practice spans enterprise strategy and strategic foresight. He is a Design Advisor to the Australian Design Council on national design capability and innovation, and co-convener, with Michael Outram APM, of the Border Futures programme.

We write in a personal and independent capacity. Our advisory relationships are disclosed at Annex A. Neither author is acting on behalf of a foreign principal. This submission is not made on behalf of any client, and no client has reviewed its contents prior to lodgement.

# 2. Strategic context: the 2026 National Defence Strategy, Integrated Investment Program and international trade facilitation agenda

The SOCI consultation must be read alongside the 2026 NDS and IIP, released by the Deputy Prime Minister and Minister for Defence on 16 April 2026, and the international trade facilitation reform agenda that is moving in parallel.

## 2.1 A broader concept of national defence

The 2026 NDS makes explicit what was previously implicit: Australian national defence now encompasses civil preparedness, fuel security, economic security and supply chain resilience. The Strategy states expressly that Australia cannot rely on access to external supply chains during a conflict; that global defence industry is already struggling to meet demand; and that 'off-the-shelf procurement no longer offers a guarantee of speed to capability'. That is a strategic judgement with direct consequences for SOCI-regulated assets, and one that places sovereign capability — the Australian ability to design, build, sustain and adapt critical systems — at the centre of national defence planning.

The consequences are structural. If the perimeter of national defence runs through ports, airports, energy and fuel systems, data centres, financial market infrastructure, food and grocery distribution and the networks that connect them, then the regulatory architecture governing that perimeter, such as the SOCI Act, the CIRMP Rules and the Ministerial Directions Powers, are no longer a specialist cyber-critical-infrastructure regime. It is part of the national defence architecture. The reforms currently under consultation should be designed with that in mind.

## 2.2 Additional funding — and explicit 'alternative financing'

The 2026 IIP commits an additional $14 billion over the forward estimates and an additional $53 billion over the decade, taking total Defence investment to $425 billion over ten years, with defence spending to rise to 3 per cent of GDP by 2033. Crucially, the IIP is delivered 'through Defence funding, estate modernisation and alternative financing where appropriate'. The phrase 'alternative financing where appropriate' is a material shift. It signals that the Government is open to structured private-sector and institutional co-investment in capability and infrastructure where the public value equation supports it.

The IIP also names counter-uncrewed air systems (C-UAS) 'to protect Australian sites, events and critical infrastructure' as a capability priority. That priority sits within the SOCI envelope and intersects directly with the physical security element of the CIRMP Exposure Draft.

## 2.3 Convergence between SOCI, NDS and IIP

The practical significance of these announcements for this consultation is threefold:

- The CIRMP Rules and the Ministerial Directions Powers are being strengthened at precisely the moment that Government has accepted that economic, supply chain and civil preparedness resilience are national defence concerns. This is the right sequence, but it means the SOCI reforms are now structurally important to a larger strategic architecture than when the 2024 amendments passed.
- The IIP's 'alternative financing' language creates a policy signal that structured co-investment models should be explored where capability uplift delivers both private resilience and public national-security value. The cost of compliance for responsible entities — particularly at the high end of the risk spectrum — is being borne as regulatory burden rather than as co-invested national capability. The reform window open today is an opportunity to change that framing.
- C-UAS and other protective technologies require co-ordination between Defence, Home Affairs, CISC, the Australian Federal Police, State police and responsible entities themselves. The Ministerial Directions Powers reform — particularly the consultation-with-affected-entities provisions — should be drafted with that multi-agency, multi-actor reality in mind.

## 2.4 The international trade facilitation dimension

Three further developments are in the public domain, each moving in parallel with the SOCI reforms and shaping the design space for this consultation.

**WTO Joint Statement Initiative on E-Commerce.** Australia co-convenes the WTO Joint Statement Initiative on E-Commerce with Japan and Singapore. The Initiative addresses, among other matters, electronic transactions, paperless trade, electronic authentication and electronic signatures — the rules-framework layer underneath digital trade.

**Australia–Singapore Digital Economy Agreement and ACCEPT.** The Australia–Singapore Digital Economy Agreement (DEA) provides a working bilateral framework for digital trade trust between two of Australia's most strategically aligned trading partners. The joint ACCEPT initiative — a digital trade facilitation trial under the DEA — has produced operational learning on cross-border data exchange, regulatory interoperability and trusted documents that is directly relevant to a SOCI-aligned regulatory sandbox.

**OECD Trade Facilitation Indicators.** The OECD Trade Facilitation Indicators (TFIs) provide an internationally comparable measurement framework for border performance across formalities, automation, governance and impartiality. They are increasingly used as the reference framework for trade facilitation reform progress globally.

These developments are not background context. They are part of the operating environment within which Australian critical infrastructure and border reform will be implemented and assessed. The SOCI reforms before the Department, and the implementation architecture we recommend in Part C, should be designed with explicit alignment to that international

architecture, both because it improves the quality of Australian reform and because Australian regulatory leadership in this space is itself a national interest.

Operationally, this points to two cross-portfolio considerations:

- The Department of Foreign Affairs and Trade (DFAT) is a necessary design partner alongside Home Affairs, CISC and Defence in the SOCI implementation phase, not a late-stage consultee. DFAT co-convenes the WTO E-Commerce track, leads on the DEA and ACCEPT, and holds the trade facilitation policy mandate. Cross-portfolio mechanisms (sandbox, co-design council) should reflect that from inception.
- Sandbox and implementation evaluation frameworks should be designed for international comparability — most directly through alignment with the OECD TFIs where applicable — so that Australian reform progress can be measured against, and contribute to, the global trade facilitation agenda.

# 3. Why the border must be treated as a critical infrastructure system

Australia's border is not a single asset. It is a system of systems spanning customs, biosecurity, migration, traveller risk management, aviation transport security and civil maritime security, operating across more than 60 seaports and airports, hundreds of authorised freight forwarders and customs brokers, the Integrated Cargo System (ICS) and many thousands of individual responsible entities. Ports and airports are already captured as critical infrastructure asset classes under SOCI. But the border as a whole — the interoperable layer that connects them — is not. That is a structural gap.

Three observations, each drawn from material already in the public domain (sources at Annex B), illustrate why this matters for the CIRMP Rules.

## 3.1 Supply-chain foreign ownership, control and influence is a system-level, not an entity-level, risk

Operation Ironside, the AFP-led international takedown of the AN0M encrypted communications platform announced in 2021, ultimately produced Operation Jardena which, as publicly reported by the AFP and ABF, identified approximately 1,000 individuals and 100 companies embedded in the Australian border supply chain with direct or close links to transnational organised crime. Those entities included freight forwarders, customs brokers, warehouse operators and transport companies — each, on its own, often a small business, but collectively forming an integrated vulnerability in the supply chains feeding every critical infrastructure asset class SOCI covers. Operation Tin Can, as publicly reported by the World Customs Organization and the United Nations Office on Drugs and Crime, extended the pattern globally across 58 countries.

A foreign ownership, control and influence (FOCI) obligation at the individual responsible entity level, as proposed in the Exposure Draft, will not by itself detect these network-level compromises. It must be designed to interoperate with a system-level visibility mechanism.

## 3.2 Physical and throughput assumptions have changed

Historical ANAO audits indicate that Australia once X-ray examined around 7 per cent of sea cargo containers. Cross-referencing that benchmark against publicly available AusTender procurement records (which show no material increase in container-examination capacity in the intervening period) and against published container throughput data, current X-ray examination of sea cargo containers can reasonably be estimated at below 1 per cent. The Australian Criminal Intelligence Commission's National Wastewater Drug Monitoring Program reports, together with associated published research, indicate that even intelligence-led targeting captures only 20–25 per cent of total illicit drug volumes entering the country. The Illicit Tobacco Commissioner has publicly estimated the illicit tobacco market at between $5.7 and $8.5 billion and foregone excise at up to $11.8 billion. The point is not that enforcement is failing in some absolute sense; it is that the throughput assumption on which our border and port infrastructure design rests has not kept pace with volume growth, and criminal and state-adjacent actors are exploiting that gap at industrial scale.

The physical security requirements proposed in the Exposure Draft are therefore welcome but partial. Physical theft, damage and sabotage are real threats. They are also connected to, and often enabled by, throughput-dependent compromise — the kind of compromise that the CIRMP regime will only catch if physical, personnel, supply chain and cyber requirements are designed as an integrated package and audited as one.

## 3.3 Data, decision-making and standards are fragmented

Consider the architectural question. If a high-risk consignment arrived at an Australian port — whether a contaminated supply chain, a foreign-controlled vendor in a critical infrastructure procurement, or a capability of future national-security concern — what would need to be true of the data architecture across agencies and responsible entities for the threat to be visible in time? Today, the relevant information sits across multiple holdings: ICS data at the ABF, cargo declarations at the Department of Agriculture, Fisheries and Forestry, intelligence at the AFP, financial-intelligence holdings at AUSTRAC, and national-security holdings at ASIO. No single system provides a unified, real-time picture; no entity sees the whole.

The Simplified Trade System (STS) was a serious attempt to address this kind of fragmentation. As reflected in successive Portfolio Budget Statements and public ANAO commentary, its scope was rescoped from transformation to facilitation. The architectural lesson must inform the SOCI implementation phase.

The fragmentation is not only domestic. The international trade and border ecosystem operates across many overlapping standards, document types and data models. Multilateral reform programmes — the ICC Digital Standards Initiative, UN/CEFACT trust infrastructure and the WTO rules framework — are now actively building the harmonised, verifiable trust layer that this fragmentation has long needed. CIRMP supply chain obligations, and the cross-portfolio architecture we recommend in Part C, should be designed to interoperate with that international standards architecture rather than to create parallel Australian infrastructure. We develop this point in S5.3.

# 4. Part A — Response to proposed amendments to Ministerial Directions Powers

The Directions Paper proposes a package of five targeted measures to enhance the Ministerial Directions Powers under Part 3 of the SOCI Act. We broadly support each of them, subject to the refinements set out below. Our starting point is that the Part 3 powers are extraordinary regulatory instruments — they can direct how a private responsible entity operates in response to a serious national security risk — and that the legitimacy and effectiveness of those powers depends on proportionality, procedural fairness and predictable industry engagement.

## 4.1 Penalty increases

We support in principle the proposed increase in maximum civil penalty exposure for non-compliance with a Part 3 direction from 250 penalty units (1,250 for corporations) to 2,000 penalty units (10,000 for corporations). At the penalty unit rate prevailing at the date of this submission (set under section 4AA of the Crimes Act 1914), this increases potential corporate exposure from approximately $412,500 to approximately $3.3 million. Given the scale of the entities captured by Part 3 and the seriousness of the national security risks contemplated, the previous cap was materially below the deterrence threshold.

Two refinements are warranted. First, the Department should publish — whether in explanatory material or guidance — the factors that will inform the Minister's and the Court's view of proportionality in applying the enhanced penalties (size of entity, materiality of risk, degree of culpability, prior engagement with CISC). Second, the penalty regime should be paired with a published review pathway, including expedited judicial review and an appropriately cleared mechanism for testing classified material where required.

## 4.2 Procedural safeguards and transparency

We strongly support the proposal to clarify consultation-with-affected-entities requirements and to require stronger documentation and oversight of decisions. This is the single most important element of the reform package. Part 3 directions are, in practice, one of the principal interfaces between the national security executive and the largest operators of Australia's critical infrastructure. If those operators cannot predict when and how they will be engaged, they cannot invest in readiness.

We recommend that the Department consider the following refinements:

- A statutory default of pre-direction consultation with the affected entity, with a narrowly drafted exception where the Minister certifies that consultation would frustrate the national security objective.
- A requirement that the Minister provide a written statement of reasons within a prescribed period after a direction is made, declassified to the maximum extent consistent with the underlying intelligence.

- Mandatory post-direction review by an independent reviewer (for example, the Inspector-General of Intelligence and Security or a dedicated SOCI reviewer) within 90 days, with findings reported to the Parliamentary Joint Committee on Intelligence and Security.
- A standing channel — through the Cyber and Infrastructure Security Centre's Trusted Information Sharing Network (TISN) or equivalent — for class-level engagement with industry on the evolving threat picture that is likely to generate directions, so that entities can invest in readiness in advance rather than respond under pressure.

## 4.3 Disclosure-delay power

The Directions Paper presents two options for handling disclosure obligations in the event of high-risk cyber incidents: Option 1 relies on ASIC's existing exemption power under section 111AT of the Corporations Act; Option 2 inserts a new SOCI-specific directions power allowing the Minister to delay disclosure for a prescribed period.

We support Option 2 in principle, but with strict parameters. A SOCI-specific disclosure-delay power has the virtue of being purpose-built for the national security context and avoids the risk of ASIC's continuous disclosure framework being repurposed for matters outside its policy intent. Our conditions are:

- A clearly time-bounded maximum delay period, set in the primary Act or Regulations, with any extension requiring fresh ministerial decision on advice from the National Cyber Security Coordinator.
- A statutory requirement that ASIC and the Australian Securities Exchange be notified of any delay decision that affects a listed entity.
- Protection for directors and officers from personal liability arising from compliance with a disclosure-delay direction, to remove the perverse incentive to disclose notwithstanding the direction.
- Transparent post-event disclosure, so that market participants can price risk accurately and so that the public interest in understanding how the regime is used is met.

## 4.4 Other measures

We support, in principle, the remaining measures in the proposed five-measure package — including provisions that improve the precision of directions and the flexibility of instruments available to the Minister. Our overarching comment is that precision and flexibility must be matched by procedural discipline. The package should be read as a whole and implemented as a whole.

# 5. Part B — Response to the Exposure Draft of the enhanced CIRMP Rules

The Exposure Draft reflects the Department's response to the first round of consultation on the Enhanced CIRMP Rules Consultation Paper (released 9 December 2025; submissions closed 13 February 2026). The Department's willingness to amend the draft in response to industry feedback — including by introducing a more calibrated physical security plan requirement and by retaining a principles-based 'as far as reasonably practicable' standard — is a positive signal. We support the general direction of the Exposure Draft and offer the following observations on each of its principal elements.

## 5.1 Foreign ownership, control and influence (FOCI)

The proposed requirement that responsible entities for high-risk asset classes identify, consider and document material FOCI risks across all aspects of their asset — including vendors in the supply chain — is an important step. FOCI is the single most under-addressed risk category in the current regime, and is directly relevant to the national defence architecture that the 2026 NDS establishes.

Our recommendations:

- The FOCI obligation should be designed to interoperate with a system-level visibility mechanism (see Part C, Recommendation 3). Entity-level documentation of FOCI risk will be fragmented, inconsistent and of limited value to national decision-makers unless it can be read at system level by CISC with appropriate safeguards.
- The Department should publish guidance on proportionality — particularly for small and medium vendors embedded in a responsible entity's supply chain — to avoid the FOCI requirement becoming a de facto barrier to market entry for SME suppliers that are low risk in practice.
- Alignment with the Foreign Influence Transparency Scheme (FITS) and the Foreign Investment Review Board (FIRB) regimes should be explicit, so that responsible entities do not face parallel and inconsistent FOCI obligations under different statutes.

## 5.2 Cyber maturity uplift

Requiring responsible entities for high-risk asset classes to comply with Level 2 of their chosen cyber maturity framework (for example, the ASD Essential Eight, ISM, NIST CSF or ISO 27001) is proportionate and long overdue. The 24-month compliance timeline is reasonable for most entities. We recommend that the Rules permit a one-off extension of up to a further 12 months, at the discretion of the Secretary, for responsible entities that can demonstrate a credible uplift plan but are constrained by legacy systems or multi-year capital cycles.

Multi-factor authentication (MFA) and AusCheck implementation requirements are supported. The Department should publish implementation guidance specific to operational technology

(OT) and industrial control system (ICS) environments, where the application of standard MFA approaches is materially more complex than in enterprise IT.

For high-risk asset classes, the cyber maturity uplift should anticipate the transition to post-quantum cryptography consistent with the Australian Signals Directorate's published guidance. The transition timeframe is long, the planning horizon overlaps with the CIRMP compliance window, and responsible entities that defer the question will face material remediation cost as cryptographic standards shift. Implementation guidance should reference the ASD post-quantum cryptography pathway and require, for high-risk asset classes, that cyber maturity plans address cryptographic agility — the ability to substitute primitives without rebuilding systems.

## 5.3 Supply chain security

The supply chain security obligation — with an 18-month compliance timeline — is the most operationally demanding element of the Exposure Draft for most responsible entities. We support the intent and offer four observations.

### Tiered supplier register

The obligation should require responsible entities to maintain a tiered supplier register that distinguishes between Tier 1 (direct), Tier 2 (sub-suppliers) and Tier 3 (further downstream) suppliers, with depth of due diligence calibrated to risk. An undifferentiated 'all suppliers' obligation will produce compliance volume without risk reduction.

### Mapped compliance with existing frameworks

The Rules should reference and build on the Defence Industry Security Program (DISP), the Hostile Vehicle Mitigation framework used in aviation and major events, and the Commonwealth Supplier Code of Conduct, so that responsible entities already operating within those frameworks can satisfy CIRMP obligations through mapped compliance rather than parallel effort.

### A trusted supplier scheme as the natural cross-portfolio entry point

The supply chain security obligation is the natural entry point for a cross-portfolio 'trusted supplier' scheme — see Part C — that could materially reduce compliance burden across SOCI, Defence industry and border trusted-trader programs.

### Alignment with the international standards architecture for digital trade trust

The CIRMP supply chain obligation will be most useful, both for responsible entities and for national decision-makers, when it can plug into the international standards architecture for digital trade trust that is now actively being built. Four reform layers — each operating in the public domain, each backed by multilateral institutions — provide the relevant scaffold:

- **GS1 standards** for product, location and party identification — the foundation identification layer used in international supply chains. GS1 Australia is an Australian-resident standards body within the global GS1 network.

- **The International Chamber of Commerce Digital Standards Initiative (ICC-DSI),** which is developing a harmonised digital trade data model in collaboration with global solution providers. ICC-DSI has been funded by the Asian Development Bank, and is now scaling with the World Bank — placing it firmly within the orbit of the multilateral development banks rather than within any single vendor or platform.
- **UN/CEFACT — the United Nations Centre for Trade Facilitation and Electronic Business —** whose work programme includes the United Nations Transparency Protocol (UNTP), Verifiable Trade Documents and the Global Trust Registry. These are not platforms. They are reform infrastructure: the trust framework for digitally-issued credentials about products, parties, locations and transactions in international trade.
- **The World Trade Organization rules framework,** including the WTO Trade Facilitation Agreement and the ongoing Joint Statement Initiative on E-Commerce — the multilateral rules underpinning paperless trade, electronic authentication, electronic signatures and cross-border data flows. Australia co-convenes the Joint Statement Initiative with Japan and Singapore.

In practical terms, a CIRMP-aligned trusted supplier scheme designed to interoperate with these layers would use GS1-based identification at the reference layer, adopt the ICC-DSI harmonised digital trade data model for supply chain documentation, and issue and consume credentials (trusted supplier, trusted trader, personnel and audit attestations) as UNTP-compliant verifiable credentials registered in or interoperable with the Global Trust Registry — all operating within the WTO rules framework Australia is helping to negotiate.

The benefit is twofold. For responsible entities, compliance burden is reduced because the same credential can be used across SOCI, Defence industry and border trusted-trader regimes, and — where bilateral or plurilateral arrangements support it — across borders. For Government, an Australian implementation that aligns with the international standards architecture contributes to, rather than runs in parallel with, the multilateral reform agenda. We recommend that the Department engage DFAT, GS1 Australia, the relevant Australian counterparts to ICC-DSI and UN/CEFACT and the cyber and supply-chain industry, in the CIRMP supply chain implementation phase to give effect to this alignment.

## 5.4 Personnel security

Expanded personnel security obligations, with an 18-month compliance timeline, are supported. Three refinements:

- The AusCheck integration should be operationalised with clear service-level commitments. Current AusCheck turnaround times are a material constraint for responsible entities in sectors with high personnel churn, particularly aviation, maritime and logistics.
- The Rules should recognise existing high-assurance vetting regimes — including Defence security clearances, ASIO Business and Government Liaison Unit (BGLU)

briefings and the Trusted Insider frameworks adopted in some responsible entities — as satisfying personnel security obligations for the individuals concerned.

- Guidance should address the Trusted Insider risk directly. Public reporting on Operations Jardena and Ironside indicates that the insider risk in critical infrastructure supply chains is both present and persistent; CIRMP obligations that focus only on initial vetting and periodic review will not address it.

## 5.5 Physical security

We welcome the introduction of an explicit physical security plan requirement in response to preliminary consultation feedback. The requirement should cover physical theft of components, damage and sabotage, and should expressly include protection against counter-UAS threats consistent with the 2026 IIP capability priority for the protection of Australian sites, events and critical infrastructure.

Two refinements:

- The Rules should specify that the physical security plan must be integrated with — not parallel to — the responsible entity's cyber, personnel and supply-chain plans. Siloed planning is the primary failure mode.
- For high-risk asset classes, the physical security plan should include a C-UAS posture statement. This does not require every responsible entity to become a C-UAS operator, but it does require each to have considered C-UAS risk and to have arrangements in place (whether self-delivered, contracted or coordinated with relevant jurisdictions and Defence) appropriate to its risk profile.

## 5.6 Compliance timelines

The staggered compliance timelines (6 months for FOCI and all-hazards; 18 months for personnel, supply chain and physical; 24 months for cyber maturity) are broadly reasonable. Our primary concern is the 6-month FOCI timeline. FOCI due diligence in complex supply chains — particularly where vendors operate across multiple jurisdictions and sub-tier visibility is limited — is not a 6-month activity for many responsible entities. We recommend extending the FOCI timeline to 12 months for Tier 2 and below, with the 6-month timeline retained for Tier 1 direct relationships.

## 5.7 Calibration by asset class

The Exposure Draft applies the principles-based 'as far as reasonably practicable' standard across hazard categories, which we support. We recommend that the Department publish asset-class-specific guidance — for ports, airports, logistics and data infrastructure in particular — to reduce the inconsistent interpretation risk that principles-based standards always carry.

# 6. Part C — Cross-cutting architecture: federated visibility, outcomes-based investment, sandbox, co-design council

This Part sets out the four architectural recommendations that, in our assessment, are required to make the SOCI reforms before the Department deliver their intended effect at system level. They are drawn from the ANU National Security College Occasional Paper (January 2026), the Border Futures Forum (26 March 2026), the 2026 NDS and IIP, and the international trade facilitation reform agenda summarised in S2.4.

## 6.1 Recommendation 3 — A federated National Border Visibility Platform (NBVP)

The NBVP, as proposed in the ANU NSC Occasional Paper, is a federated system-of-systems architecture that allows each agency and each responsible entity to maintain sovereignty over its data and operations while permitting lawful, real-time sharing and AI-supported decision-making across the system. It is not a centralised database and it is not a single agency construct. The NBVP is intended to take forward, not duplicate, the design intent of Australia's Maritime Single Window initiative — drawing on its institutional learning while addressing the cross-portfolio scope and resourcing constraints that limited that predecessor's reach.

Within the SOCI context, the NBVP provides:

- A system-level read of FOCI across responsible entities in the border-connected asset classes, enabling CISC to identify network-level risks that are invisible at entity level (see S3.1).
- A common operating picture for Ministerial Directions decisions, so that Part 3 directions are grounded in system-level intelligence rather than fragmented holdings.
- A mechanism for post-direction transparency (see S4.2), in the form of audited reporting on directions made and outcomes achieved.
- A commercial platform on which trusted supplier, trusted trader and critical infrastructure personnel schemes can interoperate — reducing compliance burden on responsible entities, and (where designed to align with the standards architecture in S5.3) interoperable with international counterparties.

We recommend that the Department commit, as part of the SOCI implementation package, to a formal scoping study for an NBVP blueprint, with industry co-design and DFAT participation, reporting within 12 months.

## 6.2 Recommendation 4 — A National Border Investment Framework (NBIF) on outcomes-based financing logic

The NBIF, also proposed in the Occasional Paper, aligns approvals and investment decisions at the border and across critical infrastructure with the national interest, driving prioritisation based on public value and national security outcomes. It is the structured complement to the IIP's 'alternative financing where appropriate' language.

Practically, the NBIF would:

- Provide a structured pathway for industry and institutional co-investment in CIRMP uplift — particularly cyber maturity, physical security and supply chain requirements — with capital deployed against measurable capability and resilience outcomes, not against compliance line items, and with verification and payment mechanisms calibrated to those outcomes.
- Create a return pathway for port, airport and logistics operators that fund border and critical infrastructure (screening facilities, kiosks, C-UAS capability, data infrastructure).
- Align approvals across FIRB, ACCC, Home Affairs (SOCI), DFAT, Infrastructure Australia and state planning authorities, reducing the multi-portfolio approvals friction that currently discourages private and institutional co-investment.
- Incorporate the procurement lessons of the Advanced Strategic Capabilities Accelerator (ASCA): co-design rather than traditional tendering, IP retention by industry participants, rapid contracting with SMEs.
- Stack with existing Commonwealth research collaboration and supply-chain resilience funding instruments, so that public capital can match private and institutional co-investment at the precompetitive end of the capability uplift curve, and so that the public-private capital architecture is designed for compounding effect rather than for parallel programmes.

The NBIF is the principal mechanism by which the SOCI reforms can shift from a compliance-burden framing to outcomes-based co-investment in national capability and resilience consistent with the 2026 IIP.

## 6.3 Recommendation 5 — A cross-portfolio regulatory sandbox with a bilateral corridor element

The Customs Act contains a regulatory sandbox mechanism under the Controlled Trials Act 2023 that is, on its face, limited to customs matters. We recommend that the Government extend this mechanism — legislatively or administratively — to permit cross-portfolio controlled trials spanning SOCI, customs, biosecurity, aviation and maritime transport security. ASIC's Enhanced Regulatory Sandbox (2020) is a direct precedent for how a sandbox can start narrow, prove the concept and expand under formal guardrails.

A practical first application would be a Brisbane 2032-anchored sandbox — directly relevant to the 2026 IIP capability priority for the protection of Australian sites, events and critical infrastructure — covering: the enhanced CIRMP Rules at port, airport and logistics corridor assets; co-investment arrangements under an NBIF design; and system-level visibility under an NBVP pilot.

We further recommend that the sandbox include, from inception, a bilateral corridor element. Meaningful trade facilitation and digital trade trust reform cannot be tested unilaterally; it requires a willing trade partner counterparty operating in the same standards architecture.

Singapore is the natural first counterparty: an Australia–Singapore corridor under the Australia–Singapore Digital Economy Agreement, building on the operational experience of the joint ACCEPT initiative, would allow CIRMP-aligned trusted supplier credentials, NBVP-mediated visibility and outcomes-based co-investment mechanisms to be tested across a real trade flow with a strategically aligned partner. The corridor element does not require the entire sandbox to be bilateral; it requires that the sandbox is designed for international interoperability from the start.

The sandbox should be:

- Industry co-designed and industry-led; government-hosted, with DFAT as a design partner alongside Home Affairs, CISC and Defence given the trade facilitation and international dimensions.
- Time-bounded (for example, 24 months) with clear evaluation criteria and an explicit fail-forward mechanism.
- Measured against an evaluation framework aligned with the OECD Trade Facilitation Indicators where applicable, to ensure international comparability and to position the sandbox as Australia's contribution to the global trade facilitation reform agenda — not solely a domestic regulatory experiment.
- Digitally backed by a 'digital policy twin' that allows participants to simulate and stress-test policy settings before committing capital. Frontex launched a digital twin initiative for EU external borders in 2024; the Johns Hopkins Applied Physics Laboratory Generative Wargaming platform is directly relevant prior art for Australian adaptation.

The sandbox should be established under formal SOCI-sector governance, with CISC as regulator of record and DFAT as co-host of the international corridor element.

## 6.4 Recommendation 6 — A standing Critical Infrastructure Co-design Council

The SOCI reforms will require sustained structured industry engagement through the implementation phase — not a single round of consultation. We recommend that the Department establish a standing Critical Infrastructure Co-design Council within CISC, drawing from the responsible entity classes, professional bodies and relevant expert advisors. Its terms of reference should include:

- Quarterly review of CIRMP implementation metrics across asset classes.
- Co-design of asset-class-specific guidance (S5.7).
- Input to Ministerial Directions procedural and transparency arrangements (S4.2).
- Oversight of the NBVP scoping study (S6.1), NBIF design (S6.2) and regulatory sandbox (S6.3), including the bilateral corridor element.
- Cross-portfolio coordination with DFAT (international and trade facilitation), Defence (NDS and IIP), the Department of Industry, Science and Resources (industry capability), the Department of Infrastructure, Transport, Regional Development,

Communications and the Arts (transport security and infrastructure), and Treasury (alternative financing and tax treatment).

- State and Territory coordination, recognising that significant portions of the critical infrastructure regulatory perimeter — including parts of the energy, water and transport asset classes — are co-regulated by State and Territory governments. The Council should provide a standing forum for cross-jurisdictional alignment on CIRMP implementation, asset-class guidance and incident response interoperability.

The Council should operate under published terms of reference, with membership disclosed, decisions minuted and outputs published — to the maximum extent consistent with national security. This would build on the existing TISN arrangements rather than replace them.

## 7. Consolidated recommendations

We recommend that the Department:

1. Finalise the CIRMP Exposure Draft substantially as proposed, subject to: (a) extension of the FOCI compliance timeline to 12 months for Tier 2 and below supply chain; (b) inclusion of an express C-UAS posture statement within the physical security plan requirement for high-risk asset classes; (c) publication of asset-class-specific guidance before the obligations commence; (d) recognition of existing high-assurance vetting and Defence-industry frameworks as satisfying equivalent CIRMP obligations (mapped compliance); and (e) alignment of the supply chain obligation with the international standards architecture for digital trade trust (GS1, ICC-DSI, UN/CEFACT, WTO) so that CIRMP-issued credentials interoperate with international counterparties.

2. Finalise the Ministerial Directions Powers amendments substantially as proposed, subject to: (a) a statutory default of pre-direction consultation with exception narrowly drafted; (b) mandatory independent post-direction review within 90 days, with findings to the PJCIS; (c) a SOCI-specific disclosure-delay power (Option 2) with time-bound maximum, ASIC/ASX notification, statutory director-officer protection and transparent post-event disclosure; and (d) published proportionality guidance on the enhanced penalty regime.

3. Commission a formal scoping study, with industry co-design and DFAT participation, for a federated National Border Visibility Platform blueprint within 12 months, as part of the SOCI implementation package.

4. Establish a National Border Investment Framework that operationalises the 2026 IIP's 'alternative financing where appropriate' language on outcomes-based financing logic — with capital deployed against measurable capability and resilience outcomes — drawing on the ASCA procurement model, and stacking with existing Commonwealth research collaboration and supply-chain resilience funding instruments.

5. Extend the Controlled Trials Act 2023 regulatory sandbox mechanism to permit cross-portfolio SOCI/customs/biosecurity/transport security controlled trials, anchor the first application to Brisbane 2032 assets and timeframes, include a bilateral corridor

element under the Australia–Singapore Digital Economy Agreement and the ACCEPT initiative, and align sandbox KPIs with OECD Trade Facilitation Indicators for international comparability.

6. Establish a standing Critical Infrastructure Co-design Council within CISC to sustain structured industry engagement through implementation, with cross-portfolio membership including DFAT, Defence, DISR (Department of Industry, Science and Resources), Infrastructure and Treasury, published terms of reference and disclosed membership.

# 8. Closing

The reforms before the Department are necessary, and well-timed. The SOCI consultation, the 2026 NDS, the 2026 IIP and the international trade facilitation reform agenda align Australia's critical infrastructure regulatory architecture with the national defence concept the Government has now adopted, and create the opportunity to position Australia as a contributor to the international standards architecture that will underpin trusted digital trade.

We respectfully submit that the Department take this opportunity to pair the SOCI reforms with the system-level architecture — federated visibility, outcomes-based investment framework, cross-portfolio sandbox with bilateral corridor element, and co-design council — without which the reforms will deliver regulatory uplift but fall short of the national-capability and international ambition the 2026 NDS, the 2026 IIP and the international trade facilitation agenda articulate. We would welcome the opportunity to engage further on any of the matters raised in this submission.

We note that Recommendations 1, 2 and 6 sit within the Department's current consultation envelope and can be progressed through finalisation of these instruments. Recommendations 3, 4 and 5 are cross-portfolio in character and will require sustained engagement across Home Affairs, Defence, DFAT, Treasury and the States. The architecture is designed to be progressed in parallel rather than in sequence.

We add one final observation. Australian regulatory leadership in this domain requires sustained engagement at the OECD, the International Chamber of Commerce, UN/CEFACT and through bilateral Digital Economy Agreement partners. The reforms before the Department, paired with the implementation architecture set out in Part C, position Australia to contribute to — and shape — the international standards and trust infrastructure agenda, rather than implement it after it is set elsewhere. That is a national interest worth pursuing on its own terms.

**Michael Outram APM**

Principal, Michael Outram Advisory; Distinguished Advisor, ANU National Security College

**Michael Eales**

Partner, Subject Matter

30 April 2026

# Annex A — Declaration of interests

We make the following declarations in the interests of transparency. This submission reflects our independent professional views. It is not made on behalf of any of the entities listed below, none of which has reviewed or approved this submission prior to lodgement.

**Michael Outram APM**

- Principal, Michael Outram Advisory (sole-trader advisory).
- Distinguished Advisor, ANU National Security College.
- Former Commissioner of the Australian Border Force and Comptroller-General of Customs (May 2018 – November 2024).
- Mr Outram operates his advisory practice in an independent capacity and continues to comply with his post-separation obligations, including under section 42 of the Australian Border Force Act 2015, Part 5.6 of the Criminal Code Act 1995, section 23 of the Foreign Influence Transparency Scheme Act 2018, the Lobbying Code of Conduct, and confidentiality obligations owed to current and former clients. His engagement terms include applicable-law compliance and confidentiality obligations binding on both parties; some engagements expressly recognise his post-separation obligations as a former Commonwealth officer.
- Declared independent advisory relationships at the date of this submission, as previously declared in the ANU NSC Occasional Paper (January 2026): Altana AI, VMI Security, TRM Labs and Sydney Airport Corporation. Mr Outram has additional advisory engagements that are subject to client confidentiality; specific entity-level disclosures are available to the Department on request.

**Michael Eales**

- Partner, Subject Matter Group Pty Ltd.
- Co-convener, with Michael Outram APM, of the Border Futures programme (industry-led, co-designed with the Copenhagen Institute for Futures Studies).
- Current or recent advisory engagements with entities across the Australian aviation, maritime, logistics, institutional capital, technology and government sectors. The Border Futures programme has engaged participants from these sectors under the Chatham House Rule; specific entity-level disclosures are available on request.

Neither author is acting on behalf of a foreign principal, and this submission is not made on behalf of any client. Our engagement with the SOCI consultation is as independent expert contributors to an open public call.

# Annex B — Source materials relied upon

All factual claims in this submission are drawn from material in the public domain. The principal sources relied upon are:

**Commonwealth material**

- Department of Home Affairs — Consultation on proposed amendments to the Ministerial Directions Powers in Part 3 of the SOCI Act; Exposure Draft of the enhanced CIRMP Rules (25 March 2026).
- Enhanced CIRMP Rules Consultation Paper (9 December 2025).
- Independent Review into the Security of Critical Infrastructure Act 2018 (Dr Jill Slay AM).
- Department of Defence — 2026 National Defence Strategy and 2026 Integrated Investment Program (16 April 2026).
- Department of Foreign Affairs and Trade — Australia–Singapore Digital Economy Agreement; ACCEPT initiative.
- Australian Signals Directorate — published guidance on post-quantum cryptography and the transition pathway for Commonwealth and critical infrastructure systems.
- Controlled Trials Act 2023 (Cth).
- Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024 (Cth).

**Parliamentary and regulatory material**

- Senate Legal and Constitutional Affairs Committee Estimates, Home Affairs portfolio (various).
- Crimes Act 1914 (Cth) section 4AA — penalty unit rate.
- Australian Criminal Intelligence Commission — National Wastewater Drug Monitoring Program reports.
- Parliamentary Joint Committee on Intelligence and Security — SOCI-related inquiries.
- ASIC Enhanced Regulatory Sandbox (2020) guidance materials.
- Illicit Tobacco Commissioner — public reporting on illicit tobacco market size and foregone excise.
- Australian National Audit Office — historical reports on cargo examination (ANAO Audit 2004-05 No.16 and successors); AusTender contract notice records on container-examination procurement; Ports Australia and Australian Bureau of Statistics published container throughput data.

### Operational and open-source

- Australian Federal Police and partners — Operation Ironside public reporting (2021 onwards).
- World Customs Organization / UN Office on Drugs and Crime — Operation Tin Can.
- Ministerial media releases and ABF newsroom material on Operation Jardena.

### International standards and trade facilitation

- World Trade Organization — Trade Facilitation Agreement; Joint Statement Initiative on E-Commerce (Australia, Japan, Singapore co-convenors).
- OECD — Trade Facilitation Indicators.
- International Chamber of Commerce Digital Standards Initiative (ICC-DSI) — published materials on the harmonised digital trade data model and ADB / World Bank programme alignment.
- United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) — United Nations Transparency Protocol (UNTP), Verifiable Trade Documents specifications, Global Trust Registry.
- GS1 international standards (identification of products, parties and locations).

### Expert and academic


- Outram, M. (2026), Beyond the Checkpoint: Managing Australia's Border as a Strategic Economic and National Security Asset in a Multipolar World, ANU National Security College Occasional Paper (January 2026).
- Border Futures Forum — Forum proceedings, Port of Brisbane (26 March 2026), Subject Matter, Michael Outram Advisory, Copenhagen Institute for Futures Studies.
- Meath, C, Karlovsek, J, Navarrete, C, Eales, M, Hastings, P (2022) Co-designing a Multi-level platform for industry level transition to Circular Economy principles: A case study of the Infrastructure CoLab, Journal of Cleaner Production.
- Outram, M. (2026), 'After the announcements, spare a thought for those who operationalise migration policy', Australian Financial Review (16 April 2026).
- Border Technology Summit ANZ keynote — 'Beyond The Checkpoint: Borders as Strategic National Assets' (24 February 2026).
- Frontex — EU external borders digital twin initiative (2024).
- Johns Hopkins Applied Physics Laboratory — Generative Wargaming platform.
- Bank of England and Payments Canada — published digital-twin / settlement-system simulation materials.


*End of submission.*