



Australian
National
University

NATIONAL
SECURITY
COLLEGE

Beyond the checkpoint

Managing Australia's border as a strategic
economic and national security asset

Michael Outram APM

About the author

Michael Outram APM is a Distinguished Advisor at the ANU National Security College (NSC) and the former Australian Border Force Commissioner and Comptroller-General of Customs. He served for 44 years in UK and Australian law enforcement and is currently an independent adviser on international border security and integrity with Altana AI, VMI Security, TRM Labs, and Sydney Airport Corporation Limited.

About this paper

Occasional Papers comprise peer-reviewed research and analysis concerning national security issues at the forefront of academic and policy inquiry. They are designed to stimulate public discourse and inform policy solutions. Discussion of technologies, data architectures or governance models is illustrative and does not constitute endorsement, commercial advice, or procurement recommendation. The author thanks the many colleagues consulted for this project but remains solely responsible for the views expressed and any errors contained therein.

Justin Burke is the series editor and Senior Policy Advisor at NSC.

About the College

NSC is a joint initiative of The Australian National University and the Commonwealth Government. The College is independent in its activities, research and editorial judgment and does not take institutional positions on policy issues. NSC offers specialist graduate studies, professional and executive education, futures analysis, and a national platform for trusted and independent policy dialogue.

ANU National Security College
national.security.college@anu.edu.au

The Australian National University Canberra ACT 2600 Australia
www.anu.edu.au

CRICOS Provider No. 00120C
TEQSA Provider ID: PRV12002 (Australian University)

Contents

04	Executive summary	
07	Introduction – what is a border?	
09	Redefining border security	
16	Border governance	
19	Federated learning systems: an architecture for modern border governance	
24	From architecture to delivery	
30	Conclusion	

Executive summary

“The challenge for the modern era is that the institutions of international order were designed for a world that no longer exists”.

Kissinger, H (2014), *World Order*.

Australia’s border extends beyond our geographic boundary. More than a line of defence, it is a strategic national asset that underpins our sovereignty, economic wellbeing, and international connection. As global military, economic, and political power continues to shift, combined with intensifying United States–China geopolitical competition, a growing intersection of national security policy and economic security policy is becoming evident at international borders.

Sanctions, tariffs and other regulatory levers are now routine features of statecraft. As well as creating new compliance pressures for legitimate traders and governments, such global turbulence generates unpredictability across borders, which in turn impacts on threat and risk identification. At the same time, transnational crime (TSOC), state-sponsored, and digital economy-based threats are converging and increasingly bypassing traditional controls.

In line with increasing volatility and uncertainty, international borders should be better equipped to handle evolving risks, complex flows of people, goods and capital, and shifting national priorities. Strategic investments in modernising Australia’s border systems would yield valuable returns in terms of risk mitigation, cross-border productivity and regulatory efficiency, and economic resilience. It would also strengthen Australia’s ability to shape regional border security frameworks and standards, build partner capacity, and reinforce our role as security partner of choice.

In this context, Australia would benefit significantly by evolving its border arrangements and enabling greater use of border-relevant data across trade, travel, logistics and financial flows through secure digital infrastructure, artificial intelligence (AI) and, crucially, an architecture that enables trust, legitimacy, and public confidence in such a system. The policy recommendations in this paper are grounded

not only in national security imperatives, but also in economic opportunity. Modernising our border requires a disciplined examination of its various operating models, digital and physical architecture, governance, and funding to deliver measurable security outcomes as well as reduced friction and transaction costs for legitimate trade and travel.

Yet the border is not treated as the national asset it is, despite generating substantial revenue through duties, taxes, user charges, and delivering critical national security outcomes. There is no systemic mechanism to reinvest those returns into the systems that enable them, and the border’s role in national security planning is not systematically embedded. As a result, many border systems are becoming outdated not only as physical infrastructure, but also in their capacity to generate demonstrable public value. Without well-planned digital modernisation, the negative impacts of geopolitical volatility, technological disruption, and global competition will be amplified at Australia’s border. The cost of inaction will be reduced public confidence, growing risk exposure, lost economic opportunity, and reduced agility in the face of disruptions and crises.

While this paper does not focus on people and immigration flows, there are still indirect implications for borders resulting from the December 2025 Bondi Beach terrorist attack, which has sharpened public expectations of what a modern security system should achieve. Where the security of individuals and risks have attributes that span multiple domains – for example, travel movements, visa status, firearms access, and prior intelligence holdings of concern – Australians will reasonably expect that risks across these domains can be integrated, assessed and acted upon across relevant jurisdictions and agencies. In contemporary risk environments, it is the sequence of data points, rather than any single indicator, that may warrant attention.

Further, the events at Bondi have reinforced the importance of border systems as part of Australia's counter-terrorism and economic security architecture. Terrorism and violent extremism are sustained not only through ideology, but through enabling networks, logistics, and finance. Illicit trade, including tobacco, generates substantial criminal proceeds and terrorism financing. This threat intersects with trade-based money laundering, sanctions evasion, and other illicit financial flows. Strengthening border visibility and cross-agency data integration therefore supports not only detection of contraband, but the disruption of higher-order national security risks.

This is not an argument for centralised surveillance or a presumption of wrongdoing, but for lawful interoperability, clear governance, and the capacity to detect and respond to cross-domain risk in a way that protects the public and maintains trust. These expectations extend naturally to the border, which remains the point at which travel, goods, capital, and intelligence-derived risk indicators converge.

This paper therefore proposes a re-think. If Australia were to treat the border as a sovereign capability, we could potentially unlock much-needed investment pathways to drive modernisation through new models of shared responsibility between government, industry, and system users. A technological and governance framework for achieving this is proposed to create a federated system-of-systems that seeks to maximise the value of data and digital infrastructure and enable a more comprehensive insight into our supply and value chains. In this model, 'visibility' is decisive in being able to understand threat and risk in near real time, in determining priorities and interventions, and in accurately evaluating their effectiveness.

By anchoring the modernisation of our border in the national priorities of sovereignty, productivity, and resilience, we would not only be better equipped to defend against future threats, but also to create sustainable public value in an increasingly contested and volatile global environment.

Ultimately, the case for this fundamental shift in how Australia conceptualises and manages its border turns on whether we want our border to be a transactional checkpoint and compliance mechanism, or a capability that is central to Australia's economic and national security. This paper argues that in today's increasingly multipolar world, Australia must transition from its traditional notions of border management to a far more systematic and integrated approach.

Key Points

- Borders have become important instruments of economic security, national security, and statecraft where threats converge and policy is enlivened.
- Australia's border generates substantial public value but is under-leveraged, fragmented in governance, and weakly embedded in national security planning, with consequences for effectiveness, investment, and public confidence.
- Borders are high-volume/high-ambiguity risk environments where visibility across supply chains and traveller pathways is a decisive attribute of effective border governance, management, legitimacy, and policy effectiveness.
- Traditional, siloed border operating models cannot scale quickly enough to balance the management of contemporary threats with trade and passenger volumes and economic security demands.
- Enhanced/new federated digital systems offer a realistic pathway for border modernisation, enabling shared visibility, AI-supported decision-making, and coordinated action without centralising control.
- Sustainable border reform requires a well-governed and staged approach, embedded within national strategy and supported by sustainable funding and co-investment models, delivering a durable capability but also positioning Australia to shape regional approaches as a security partner of choice.

Recommendations

The following recommendations build on the analysis in this paper to establish Australia's border as a strategic economic and national security asset. They propose a unified strategy, enhanced governance, modern technology, and cross-cutting collaboration to protect Australia's economy and security. They are grouped thematically to highlight priority areas, and their numbering reflects the order in which they are developed in the body of the report.

Strategy

Recommendation 1 (p.10) – Develop a National Border Strategy to unify efforts across economic and national security, national resilience, and supply chain sovereignty; anchored in a coherent national vision and aligned with Australia's long-term interests.

Recommendation 4 (p.18) – Review national security priorities to ensure maximum value is obtained from the border, ensuring coherent oversight, accountability, and strategic alignment across Australia's national priorities.

Recommendation 6 (p.24) – Review border-related legislative and policy frameworks that underpin the design of digital systems; to preserve data sovereignty, protect privacy, uphold public trust and enable system-wide data sharing, interoperability, and coordinated decision-making.

Recommendation 7 (p.27) – Conduct a national program of public research to strengthen public confidence and legitimacy for border modernisation by assessing community perceptions, expectations, and trust thresholds concerning the use of data, digital infrastructure, and AI-enabled decision support.

Governance

Recommendation 3 (p.18) – Establish an Expert Advisory Board to develop the National Border Strategy, including the adoption of AI, harnessing data, regulatory innovation, and horizon scanning. The board should include selected representatives from industry, academia, and key departments and agencies to ensure both innovation and practicality; supporting and informing key decision-making bodies.

Recommendation 8 (p.28) – Establish a National Border Coordination Committee, bringing together the heads of key departments and agencies (drawing on the Expert Advisory Board as required) to shape standards, prioritise risk, and oversee the implementation of a strengthened federated border.

Implementation

Recommendation 5 (p.22) – Design a blueprint for a National Border Visibility Platform as the digital backbone of cross-portfolio border governance, enabling shared situational awareness, policy implementation and performance monitoring, coordinated prioritisation and timely operational decision-making. Working under the leadership of the Expert Advisory Board, and building on the Simplified Trade System reform, this platform should incrementally replace the Integrated Cargo System and lawfully share data across government and industry.

Recommendation 9 (p.29) – Establish a National Border Investment Framework to align approvals, investment decisions and the national interest, supporting the transition from episodic risk treatment to embedded system-wide assurance. The framework should drive prioritisation based on public value and national security outcomes under the oversight of the National Border Coordination Committee.

Recommendation 2 (p.14) – Conduct annual border resilience exercises to test national preparedness, inter-agency coordination, and systemic response to both anticipated and novel disruption scenarios at the border.

Introduction – what is a border?

“National and economic security are more closely intertwined than ever as Australia grapples with a world of permanent churn and change.”

Dr Jim Chalmers, Treasurer of Australia, National Press Club address, 4 June 2025.

With 34,000 kilometres of coastline and an ocean territory spanning 8.2 million square kilometres,¹ as well as 31 designated international airports,² and 39 international seaports of entry,³ Australia's border is vast, complex, and exposed.

Our border is a dynamic system that connects us to the world while safeguarding our sovereignty, economy, and society. In a valedictory address at the National Press Club in 2024, I argued for border governance to evolve from a reactive enforcement frame to that of a strategic national asset, shaped by foresight, orchestrated investment, and deeper inter-agency coordination.⁴ Today, the case for that shift is far more pressing with globalisation and the global trading system as we have known them increasingly breaking down⁵ and strategic competition intensifying.

The arguments for change that are put forward in this paper are marked in many ways by the weaponisation of trade, technology, and supply chains. The response of several other countries underscores this point; the United Kingdom's *Integrated Review Refresh* (2023)⁶ warns of these systems being increasingly used as tools of statecraft, and Japan's *National Security Strategy*⁷ identifies vulnerabilities such as economic coercion and supply chain fragility as being major security challenges and systemic risks within its expanded conception of national security.

Australia likewise relies on access to global markets, open and safe trade routes, and fast, frictionless supply chains. Meanwhile, the systems that underpin the global movement of goods, people, capital, and data are now more contested and fragile than at any time since the Second World War. International borders, the connective tissue between these systems, have become theatres of contest: from cyber

interference against critical systems and sanctions enforcement to trade embargoes; from critical goods chokepoints to the conveyance of grey zone threats. The question is not only whether the border matters across these domains, but whether our institutions can keep pace with its evolution.

For a country so dependent on Indo-Pacific trade flows, secure sea lanes and critical imports, Australia's border is much more than a compliance checkpoint. It is where national security, economic resilience, and sovereign decision-making should converge if we are to uphold our values and norms against a tide of geopolitical change. How effectively we preserve and harness our connections with the world through trade and travel will determine whether Australia's economic advantages are sustained or lost.

Viewed this way, beyond its important role in preventing biosecurity risks and illegal migration, our border has effectively become a strategic economic and national security asset by default rather than design. But harnessing its full value as such would require disciplined investment in its maintenance, modernisation, and governance.

Decades of relative global stability, globalisation, and a rules-based trading environment have allowed border management to operate largely as discrete transactional functions focused on facilitation and supported by targeted, risk-based compliance and enforcement. This model worked well and delivered significant efficiencies, reflected in machinery of government changes such as the consolidation of the Australian Quarantine and Inspection Service within the Agriculture portfolio, the establishment of the Anti-Dumping Commission within the Industry portfolio, and the establishment of the Australian Border

Force (ABF) as an integrated customs, immigration and civil maritime security agency within Home Affairs.

These arrangements were designed for a more stable and predictable global environment and are increasingly being strained by a new set of conditions. Functional separation can limit coordination in planning, investment, and system design, reducing the border's effectiveness as a strategic policy lever; whether responding to crises, emergent shifts in national priorities, or supply chain disruption.

A modern border system can contribute more directly to prosperity and resilience by creating shared visibility, reducing friction and risk in cross-border trade and travel, enabling smarter risk-based regulation, and directing finite resources to where they have the greatest effect. While the border should not be seen as catch-all for managing all aspects of trade, travel, and technology flows, it can provide policy-makers with greater visibility, clearer lines of sight for risk owners, and intervention options that have greater precision and scale.

In the absence of a coordinated approach to planning and reinvestment in border capability, the effectiveness and capacity of Australia's border to deliver security, efficiency, and economic outcomes steadily erodes. Departments and agencies continue to invest within their individual mandates and budget appropriations, with no system-level mechanism to align priorities, sequence investment or achieve phased modernisation.

The *Aviation White Paper – Towards 2050* (2024)⁸ recognises aviation as being critical to Australia's way of life and anticipates sustained growth in passenger and cargo volumes. It acknowledges the need for ongoing investment in border security and facilitation, and signals a future vision for a more digital, contactless, and secure border environment.

While necessarily aviation-specific, the White Paper reflects a broader shift in how nationally significant systems are being understood as interdependent arrangements, which require coordinated governance, long-term investment and clear oversight. Considered in this light, the border is not simply a collection of modal or portfolio-based responsibilities, but a national capability in its own right.

In practice, the border brings together customs, biosecurity, migration, traveller risk management, aviation transport security, and civil maritime security, and connects directly with adjacent domains such as the digital economy, financial intelligence, and supply chain visibility. In recent decades, however, national attention in Australia has tended to concentrate more narrowly on immigration and maritime enforcement, particularly Operation Sovereign Borders.

At the same time, the economic consequences of biosecurity breaches, whether to livestock, crops, or native ecosystems, continue to underscore the critical role our border plays in safeguarding agricultural exports and economic wellbeing. These roles are interdependent and require a broader approach to border governance that is integrated, anticipatory, and adaptive.

Today's more turbulent and unpredictable global environment is placing new demands on border systems globally, requiring greater agility and foresight. These are no longer discretionary enhancements, but core requirements for national resilience. Achieving them requires deliberate, long-term planning to manage complexity and enable effective whole-of-government coordination.

To maximise the public value derived from the border, and from the investments made in it, the border can be reimagined as a national governance platform capable of providing system-level visibility to inform policy and support coordinated action. Framed this way, the border can deliver assurance across the system and equip decision-makers with the tools they need to manage risk with greater precision and confidence.

This paper considers how future operating models, supported by data and digital infrastructure, AI-enabled decision support, strengthened cross-portfolio coordination, and new investment approaches could be used to build a modern border that supports Australia's national interests, every day and in crises. It also envisages a border that commands public confidence and is capable of managing increasingly complex and dynamic risks over time.

Redefining border security

“Borders have profound political and economic importance.”

Helen V. Milner, (2016), “Do Borders Play an Economic Role?”, *Les Rencontres Economiques*.

Borders can no longer be simply defined as barriers, checkpoints, or interdiction activity. In an era of economic coercion, sanctions, and strategic competition their strategic value lies in their ability to operationalise national security policy through trade, data, and regulatory controls. The effectiveness of modern sanctions regimes – including those imposed following Russia’s invasion of Ukraine – now depends on customs systems, shipping data, trade documentation, provenance visibility, and financial transparency, much of which sits at, or upstream of, the border.

Borders have evolved to become economic control systems through which states give operational effect to national security, foreign policy, and economic objectives. The challenge for governments, therefore, is to look beyond the arrival of people and goods at the physical border and manage a border continuum that begins where goods, travel, and migration originate. Border risk management is now about far more than physical inspection; it includes being able to reconcile complex and sometimes contradictory data across global trade and travel systems.

Sanctions enforcement and borders – Russian oil (2022-2025)

Since Russia’s invasion of Ukraine in 2022, Australia has imposed sanctions on Russia’s energy exports⁹ as part of a coordinated international response aimed at restricting revenue flows and degrading Russia’s warfighting capacity. Beyond diplomatic intent, the effectiveness of these instruments depends on the capability of border systems to verify origin, ownership, routing, and financial settlement across global supply chains.

Independent analysis by the Centre for Research on Energy and Clean Air (CREA) indicates that substantial volumes of Russian crude continue to reach global markets after being refined in third countries and re-exported as petroleum products. This reflects a sanctions evasion typology that involves blending, trans-shipment, refinery origin rules, layered ownership structures and the use of cryptocurrency-based payment mechanisms, which complicate enforcement.¹⁰

The CREA estimates that since 2023, Australia has imported several million tonnes of refined petroleum products derived from Russian crude. While the precise quantum is contested, the case demonstrates the difficulty of establishing provenance through shipping data, trade documentation, and refinery-based origin rules alone.¹¹

In November 2025, the Australian Senate referred the effectiveness of sanctions against Russia to a Senate committee for enquiry. Evidence provided during Senate Estimates has also clarified the structural limits of current border enforcement arrangements, with officials noting that while customs systems are designed to assess compliance at the port of import, sanctions enforcement involves refinery origin rules, beneficial ownership, and complex commercial settlement arrangements that often sit beyond the operational remit of border agencies.¹²

Taken together, the elements of this case illustrate a defining feature of contemporary border management: when national security policy is pursued through economic and trade-based instruments, the border becomes the primary operational arena in which that policy is enforced. Its success relies heavily on the capacity of border systems to provide visibility; where that capacity is limited, even high-priority policies risk being undermined before goods reach the physical border.

Multiple reform efforts have occurred in recent years that span border infrastructure, biosecurity, migration, and trade. For instance, the Simplified Trade System (STS),¹³ a microeconomic reform established within the Trade portfolio with oversight from a tripartite ministerial group. While STS governance arrangements reflected a broad recognition of the need for reform, progress has been difficult to sustain over time. Beyond the portfolios of its three sponsoring ministers, limited attention was given to aligning policy intent, funding, and sequencing across government.

Australia's economic prosperity and security are heavily dependent on open maritime and aviation trade routes, including for critical goods that move through complex global supply chains.¹⁴ There is an inherent tension between maintaining economic openness and increasingly robust risk management at our sea and airports, and that tension is increasingly being exploited, with some states seeking to leverage dependencies in global transportation and financial systems.¹⁵ Those same systems are also where vulnerabilities in critical infrastructure, cyber networks, and dual-use commercial technologies intersect, further raising the stakes for how the border is governed and secured.

Identifying and mitigating risk, as far offshore as possible, is now an accepted expectation of modern border management. Meeting that expectation will increasingly demand an approach that surfaces risk within the vast amounts of data generated across traveller and goods flows. This is particularly important at the seams between systems, actors, and jurisdictions, where regulatory gaps create the greatest opportunity for criminal arbitrage and grey zone activity. Achieving this demands more than piecemeal enhancements.

The border is better understood when viewed as a dynamic interface where global value chains (discussed at Section 3.1), contested geopolitical environments and emerging threats converge. Many contemporary risks, including organised crime and modern slavery, depend on being hidden within legitimate trade and travel channels.

Increasingly, global supply and value chains are also being used by states, and their criminal proxies, to undertake nefarious activity and obscure attribution, circumvent sanctions,

or exert economic or political power beneath the threshold of armed conflict. Grey zone activity falls between the traditional war and peace duality and often involves ambiguity and opacity of the parties involved.¹⁶ Its use has been regularly flagged by European security and intelligence leaders and demonstrates how borders have become central arenas for economic coercion, regulatory arbitrage, and strategic competition.

Delivering coherence across such a system, through coordinated governance, foresight, and enforcement, is no longer solely about efficiencies. It is central to improving system performance and assurance, and to strengthening Australia's future national resilience by:

- improving economic performance through smarter, more agile processes that reduce friction for low-risk trade and travel while focusing compliance effort where it matters most
- aligning economic, foreign and national security policy in key areas by ensuring that instruments such as free-trade agreements, sanctions, export controls, and supply-chain integrity can be monitored and implemented effectively at the border
- keeping pace with cross-border threats that are increasingly diffuse, digitally enabled, and deliberately ambiguous.

The case for having a long-term strategy for our border, on both economic security and national security grounds, continues to strengthen. The development of such a strategy is a key recommendation of this paper.

A border strategy

Recommendation 1

Develop a National Border Strategy to unify efforts across economic and national security, national resilience, and supply chain sovereignty; anchored in a coherent national vision and aligned with Australia's long-term interests.

A border strategy is a central mechanism through which governments give operational effect to economic security policy, whether protecting critical supply chains, enforcing sanctions, or responding to coercive trade measures. As economic security policy

increasingly relies on trade, investment, and supply-chain controls, the border becomes a point at which such policy can succeed or fail in practice.

Australia's border, along with its infrastructure and systems, are critical for our economy, with immense volumes of trade, travel, and data flowing each year. In 2021–22, Australian ports handled over 8.6 million TEU (Twenty-Foot Equivalent Unit) containers,¹⁷ the Integrated Cargo System (ICS), Australia's 25-year-old digital cargo platform, processed more than 1 billion transactions, and international trade in goods and services exceeded A\$1.2 trillion¹⁸. These volumes highlight the nature of the challenge for Australia's border agencies, and the forecast is for ongoing growth in trade and travel volumes, a demand for more speed and less regulatory friction, and a worsening threat outlook. Just as prosperity crosses our border and into our economy, so do supply chain risks, international obligations, and geopolitical pressures.

This has significant implications for how the border is governed and modernised, and for the level of assurance Australia can realistically achieve under current operational settings. To illustrate this point, the ability to X-ray sea cargo containers remains an important but inherently limited component of border risk management. It occurs at the point of import and is applied to a very small, targeted subset of containers. Whilst this operating model delivers significant operational outcomes, it was never designed to provide assurance across Australia's increasingly complex supply chains.

As trade volumes, regulatory complexity and threats continue to grow, a border operating model that relies heavily on such low physical inspection coverage at the point of arrival, however well targeted, cannot deliver the level of visibility and confidence now required. The challenge here is one of system design: aligning the operating model, digital infrastructure, and policy settings to manage risk across the entire border continuum.

The cumulative cost of goods and people crossing borders can be substantial. Intermediate goods often transit several jurisdictions, and each step adds friction through regulatory barriers, compliance obligations, and layered

documentation. Without effective facilitation, these costs compound and, in the case of trade, are described by the OECD as producing a tariff amplification effect.¹⁹ As more stringent passenger controls and visa requirements are introduced, a similar dynamic is becoming evident across traveller pathways.

But it is possible to mitigate many of these inefficiencies even in today's more turbulent environment, provided we have good visibility across our supply chains and traveller pathways. As a practical example, the Australian Trusted Trader (ATT) Program²⁰ could be significantly scaled and modernised through stronger digital risk stratification to better reflect differences in risk across goods and routes and the role, behaviour, and compliance maturity of the entities being accredited.

Such a model would enable clearances to be increasingly automated for demonstrably low-risk operators, with regulatory and enforcement intervention being focused on traders, supply chains, and intermediaries that present high or uncertain risk. Whilst lowering friction for compliant trade, this would also strengthen system-wide assurance.

A border can also be configured to reduce a nation's vulnerability to economic coercion, including tariffs, trade embargoes, and disruptions in critical supply chains. Australia's experience in 2020, when China imposed punitive trade measures across key export sectors, revealed how asymmetric economic coercion exploits opacity, concentration, and dependencies within global trade. Australia mitigated the impact by redirecting exports and building new markets, but analysts have since warned that resilience may be more strained under future, more coordinated or sustained coercive action.²¹

Responding in such circumstances takes time, coordination and policy flexibility. Border capability has a role to play because it is the point at which trade policy, market access, regulatory controls, and supply chain intelligence are given operational effect. Real-time supply and value chain visibility enable earlier detection of risk exposure, more precise calibration of responses, and faster policy implementation, whether that involves rerouting trade, managing exemptions or compliance requirements, supporting diversification,

or enforcing countermeasures. In turn, this demands an adaptive border system with real-time data and intelligence-sharing capabilities.

However, such an approach is constrained by current thinking, operating models, legacy systems, loosely coordinated governance, and siloed reforms. Without a unifying, future-focused approach to modernising our border as a system, ambitious reform initiatives such as the STS may continue to stall or deliver partial benefit (discussed further at Section 3.1).

Comparable jurisdictions are taking the initiative in various ways; data legislation, operational AI, and national security screening are all being advanced, but the direction of travel is consistent. For instance, the UK's *2025 UK Border Strategy*²² explicitly treats the border as a platform for economic resilience, national security, and data-driven governance, describing “data sitting at the heart of the operation of the border” and committing to new border data legislation to allow for more effective sharing of information between public and private entities. Singapore is introducing AI-assisted border screening and is integrating its digital architecture with new port infrastructure.²³ The US²⁴ and Japan²⁵ have codified supply chain resilience and dual-use technology screening as being central to their national security strategies. Without a comparable shift, Australia risks falling behind by treating our border as a bureaucratic perimeter, while others leverage theirs as a source of strategic advantage.

Economic security considerations within a border strategy

As economic security becomes more central to defending sovereignty, managing critical dependencies and projecting influence, its integration with national security is being institutionalised across many major economies. Japan's *Economic Security Promotion Act* prioritises technological sovereignty;²⁶ the EU's *2023 Economic Security Strategy*,²⁷ South Korea's *National Security Strategy*,²⁸ and the UK's dual-use screening and investment controls²⁹ reflect similar shifts. In the US, economic tools ranging from supply-chain controls to investment screening have become central to the *National Security Strategy*.³⁰ Many of these strategies necessarily

focus on specific industrial sectors, classes of asset, and technologies. However, they can overlook the infrastructure through which risk is transmitted, such as air and seaports, and associated logistics networks.

It follows that modern, well-managed, borders are critical to the success of economic security strategies. But they often remain underleveraged and, as economic security policies move towards implementation, governments are increasingly compelled to focus on operational levers that deliver the greatest impact. Gaining earlier visibility and greater control over the movement of goods, people, and data crossing the border is therefore central to effective economic security policy. While such measures may sometimes be perceived as protectionist, they are a necessary response to global volatility, coercion and strategic competition.

In recent years Australia has established the Office of Supply Chain Resilience, developed strategies around critical minerals and critical technologies, enhanced foreign investment scrutiny, and established the Cyber and Infrastructure Security Centre (CISC). These are all important steps in strengthening our economic security, but they appear largely unconnected. It is also noteworthy that the border is not integrated within the governance frameworks that underpin these initiatives and that without such, we are unable to develop the border to its full potential as a strategic economic and national security asset. This paper returns to this theme in Section 5.

Developing the border as a platform for economic statecraft requires designing it in ways that translate Australia's broader policy goals into operational effect. To do so would involve creating:

- real-time visibility across the system
- intelligence-led, cross-agency regulation and enforcement
- alignment of trade, investment, and security controls.

Put simply, the border must shift from managing flows to proactively shaping them in Australia's economic interests.

The threat environment factored into a border strategy

The complexity and ambiguity of the threats at our border are unprecedented in the modern border management era, and the outlook is generally worsening. Nor are traditional risks such as people smuggling or drug trafficking reducing. In addition, the strategic manipulation of global supply chains requires attention as state and non-state actors exploit regulatory gaps, digital vulnerabilities, and jurisdictional complexity to exert influence and evade detection.³¹

Data networks, digital financial systems, and legal loopholes are being used to transfer money, technology, and influence across borders undetected. Even the risks posed by shipping containers are changing,^{32,33} dual-use technologies, cyber-physical devices, and remote-operated platforms are blurring the distinction between licit and illicit flows.

The crypto economy is further complicating this picture, with criminals being enthusiastic adopters at scale. Global cryptocurrency market capitalisation exceeded US\$3.5 trillion in the second quarter of 2025,³⁴ underscoring its rapid emergence as one of the world's largest financial ecosystems. This expansion has effectively pushed the financial system's perimeter beyond the reach of traditional regulatory methods.

Relevantly, the United Nations estimates that 2–5 per cent of global gross domestic product (GDP) is laundered annually,³⁵ with a material share of that activity being trade-based money laundering (TBML). TBML involves disguising illicit proceeds through the misrepresentation of trade transactions, such as falsified invoices, over- or under-valuation of goods, and phantom shipments. It remains an enduring risk for customs and border management because it exploits systems designed to facilitate legitimate trade.

To put the scale of this challenge into an Australian perspective, the Illicit Tobacco and E-Cigarette Commissioner (ITEC) estimates

that the combined illicit tobacco and e-cigarette market in Australia is worth between A\$5.7 billion and A\$8.5 billion annually, with foregone excise revenue estimated at up to A\$11.8 billion in 2024-2025. This places illicit tobacco and vaping products among the country's largest single sources of criminal proceeds.

While precise data is limited, it is reasonable to assume that a significant share of these profits is retained by TSOC groups and laundered through a combination of cash-based activity, underground banking, and increasingly digital value-transfer methodologies. Separately, international typologies and reporting now point to an emerging risk;³⁷ the ability of criminal networks to convert cash into crypto-assets, move value offshore outside regulated financial systems, and use those assets to settle payment for otherwise legitimate goods that are subsequently able to be imported to Australia or other countries. This form of crypto-enabled trade-based money laundering does not replace traditional TBML techniques, rather, it allows the financial settlement layer to be hidden from regulatory reach. It also exposes a critical gap between financial surveillance and border management systems, complicating detection and challenging border risk and targeting models.

Notwithstanding the threat picture, what is clear in practice is that border agencies are required to live within their means. In an environment of ongoing fiscal pressure and competing national priorities, simply employing more officers or undertaking more physical inspections of cargo is not the answer. The limiting factor is not effort or intent, but the operating model.

While current figures on container examination coverage are not published in consolidated form, historical audits provide a useful benchmark. An Australian National Audit Office (ANAO) report in 2004-05³⁸ found that Customs was able to examine up to around 7 per cent of sea cargo containers, at a time when total container volumes and supply chain complexity were a fraction of today's levels.

Since then, containerised trade volumes and supply chain throughput have increased dramatically,³⁹ while container examination capability has not expanded at anywhere near the same rate. On a conservative order of magnitude basis, this suggests that well below one per cent of inbound sea containers are now subjected to an X-ray examination. This is not a criticism but a structural constraint, in that inspection capacity has not scaled with trade volume. The policy question, therefore, is not only whether border agencies are able to target effectively within this constraint, but whether the constraint is strategically tenable.

If that constraint is accepted, border management becomes compelled to shift even more quickly towards earlier and more precise management of risk. Being able to monitor, respond to, and anticipate the threat landscape demands agile systems, real-time data sharing, collaborative targeting, and ongoing

analytics that can detect anomalies, trace origin points, and help to neutralise threats before they materialise. Traditional models of border risk management will not serve Australia well in the coming years, with waves of layered, ambiguous, and fast-moving threats heading our way. Success depends very much on our ability to see, understand, and respond in real time.

Border preparedness and resilience

Recommendation 2

Conduct annual border resilience exercises to test national preparedness, inter-agency coordination, and systemic response to both anticipated and novel disruption scenarios at the border.

Spotlight: emerging threats and exercise scenarios

Autonomous submersibles and ‘black flights’

Small, uncrewed aerial and maritime platforms are increasingly being used to transport illicit goods and people across borders. In bypassing established surveillance and enforcement infrastructure, they complicate attribution, interdiction, and deterrence.

Containerised weapon systems and dual-use cargo

Military-grade payloads can be concealed within otherwise legitimate commercial cargo. Ukraine’s Operation Spiders Web revealed how such systems may be pre-positioned within adversary territory, exploiting under-screened supply chains and commercial transport routes.

Crypto-enabled Trade-Based Money Laundering (TBML)

As the crypto economy grows, criminal networks are increasingly able to obscure ownership, origin and purpose of cross-border transactions. When combined with trade, this enables illicit value to be laundered through legitimate goods movements with limited visibility.

Cyber-physical systems embedded in trade

Legitimate goods, including Internet of Things-enabled machinery, software-defined tools, and dual-use components may be exploited for sabotage, surveillance, or disruption of border operations and critical infrastructure, often without detection until operational use.

Effective border strategy requires foresight and preparedness. Prior to the COVID-19 pandemic, Commonwealth and state agencies conducted a desktop exercise based on a pandemic/Australian port scenario, but in the absence of the ABF or Home Affairs. When the *Ruby Princess* cruise ship arrived in Sydney during the pandemic, gaps in shared assumptions, rehearsed coordination, and clear accountabilities were laid bare. A Special Commission of Enquiry⁴⁰ and subsequent reviews found fragmented coordination and unclear accountabilities, underscoring the consequences of inadequate preparedness. These lessons are directly relevant to contemporary border risks where complexity, ambiguity, and cross-cutting dependencies are the norm.

There is a strong case for regular testing of Australia's border preparedness. Current and emerging threats are sufficiently serious to warrant assumptions about data access, decision authorities, and coordination mechanisms being tested before crises occur. These threats generate border risks characterised by complexity, ambiguity, and cross-cutting dependencies that cannot be resolved in real-time during a crisis. Annual, cross-jurisdictional border resilience exercises provide a practical way of doing so, strengthening readiness, clarifying accountabilities, and informing national risk planning.

Border governance

“The post-Cold War world is over, and a new era of geopolitical competition is under way.”

Jake Sullivan, US National Security Advisor (2023), Remarks at the Brookings Institution.

From the end of the Second World War until recently, trade was largely stable and open, under the auspices of multilateral economic structures including the International Monetary Fund, the World Bank, and from 1995 the World Trade Organization. It followed logically that the role of customs at the border be streamlined to facilitate the efficient and open movement of goods. Border infrastructure, technology, and regulation were also designed to support globalisation.

A sequence of events revealed vulnerabilities in this system including 9/11, the 2008 Global Financial Crisis, the emergence of China's Belt and Road Initiative, and the COVID-19 pandemic. Today, that system of rules is fracturing⁵ and rivalry between the US and China has turned trade into a geopolitical contest.

Trade wars, economic sanctions, export controls, and restrictions on critical minerals and dual-use technologies are now commonplace. They are also elevating the importance of border management in supporting national strategy. Border operations should ideally enact, with precision and speed, the intent of national policy and policy changes. This applies on a day-to-day basis and for larger policy shifts, such as responding to sudden changes in tariff rates, ensuring compliance with trade agreements, or implementing digital sovereignty frameworks such as the European Union's General Data Protection Regulation (GDPR).⁴¹ Consequently, governments and industry alike are increasingly concerned about compliance pressures and need a higher degree of assurance about what exactly is crossing their borders and supply chains, and why.

Previous sections in this paper have made a case for Australia to modernise its border as a strategic platform for economic and national security benefits. With relevant responsibilities being split across portfolios, legacy systems that are ill-suited to real-time threat environments, and cross-sector coordination being largely ad hoc, commissioning work to examine the benefits of integrated gover-

nance and fit-for-purpose digital infrastructure appears sensible. It is not a race, but it is worth asking whether Australia risks being outpaced by other comparable nations that are already treating their borders as engines of geopolitical leverage, technological innovation, and supply chain control; and whether it matters.

Widening the aperture

Much of today's approach to managing the border remains based on long-held assumptions from a previous era; uninterrupted trade, stable geopolitical relationships, and narrow compliance mandates. We prioritise volumetric throughput and administrative efficiency, which is unsuited to a world drifting quickly towards strategic ambiguity, geopolitical turbulence, and protectionism. That drift is also bringing more economic coercion, supply chain disruption and grey zone threats into the frame. To cope, a modern border has to function as an integrated system that can see, think, and act across border domains and threats. Without change, our visibility remains siloed, our collaboration reactive, and our national priorities interpreted differently across portfolios.

Gaps in connective governance are evident across many cross-cutting aspects of border management, resulting in missed opportunities and requiring industry to navigate multiple, often disjointed, regulatory touchpoints across government. The STS, intended to remedy some of these issues, was designed and introduced in the 2020/21 Budget. It is a high-potential reform, but by the end of my tenure as ABF Commissioner, in late 2024, it had made little progress. The STS was ably led by the Trade portfolio, in collaboration with Home Affairs (ABF) and Agriculture. It aims to streamline and modernise cross-border trade, including the replacement of the ageing Integrated Cargo System (ICS) with a modern “single-window” digital platform. It was an ambitious undertaking with over 32 federal agencies, 145 ICT systems, and more than 200 regulatory instruments in scope.⁴²

However, the STS reform lacked central delivery authority. There was no driving role for the Department of Prime Minister & Cabinet (PM&C) or the Treasury, and it sat outside the oversight of the Secretaries Committee on National Security. Whilst a cross-government taskforce was established within the Trade portfolio, without institutional backing from the central departments, it gained limited authority and momentum. In 2024 the STS Taskforce was absorbed into Austrade. Over time the original ambition was reduced, from whole-of-border transformation to modified trade facilitation; the latter being more

suited to the bygone era of stable trade and globalisation.

This highlights a broader governance gap. Australia lacks a standing mechanism responsible for maintaining a systems view of the border over time. Without such a function, even the most promising border reform initiatives are vulnerable to portfolio capture, loss of momentum, and a gradual narrowing of ambition as priorities shift. Exercises and reforms may occur, but their lessons are not consistently retained, integrated, or translated into the ongoing system design.

From disruption to insight

Operation Jardena⁴³ was conceived with a deliberately different purpose to many earlier border taskforces. While it involved targeted operational activity, its primary objective went beyond interdiction or prosecution. Jardena was designed to treat operational activity as a means of generating intelligence about how the border system itself was being exploited, and how policy, regulatory settings and operating models might need to change as a result. In that sense, operational disruption and system learning were equally important outcomes.

Seizures and arrests mattered, but so did understanding how criminal groups had embedded themselves within legitimate trade flows, how border controls were being circumvented, and why intelligence and risk systems had failed to surface these vulnerabilities earlier. Jardena functioned as both an enforcement tool and diagnostic exercise, deliberately probing the border as a system.

Unlike many earlier taskforces that delivered important tactical outcomes without enduring change, Jardena was explicitly border-centric and grounded in customs authorities under the Customs Act, operating in close coordination with the Australian Federal Police and other domestic partners. Its focus extended beyond individual offences to the trade, logistics, and financial mechanisms that enabled illicit activity to thrive at scale, and it fed those insights back into operational, compliance, and policy settings.

Crucially, Jardena revealed that many of the risks confronting Australia's border were systemic and transnational. The vulnerabilities being exploited were shaped by global supply chains, uneven regulatory regimes, and fragmented data visibility, and could not be addressed through domestic enforcement alone.

These insights directly informed the development of Operation Tin Can,⁴⁴ which extended Jardena's logic into a multi-lateral context through the World Customs Organization and engagement with key international partners. Tin Can demonstrated how border agencies, industry, and international counterparts could lawfully combine data, intelligence, and operational insights to detect risk earlier, disrupt criminal networks further upstream, and improve targeting accuracy and the precision of physical inspections at the border.

What was missing, however, was not operational success, but an enduring mechanism to retain insight, drive reform, and translate learning into sustained capability. Like earlier taskforces, Jardena and Tin Can were time-limited. This underscores a central lesson for modern border management: lasting strategic impact does not emerge from episodic enforcement surges, but from capturing learning and translating operational experience into system reform. Without this, even successful interventions deliver only temporary gains.

Governing the border as a system

Recommendation 3

Establish an Expert Advisory Board to develop the National Border Strategy, including the adoption of AI, harnessing data, regulatory innovation and horizon scanning. The board should include selected representatives from industry, academia, and key departments and agencies to ensure both innovation and practicality; supporting and informing key decision-making bodies.

To sustain reform, Australia needs an enduring mechanism to retain institutional learning and apply it over time. An Expert Advisory Board would provide that continuity, linking subject matter expertise and operational insight to strategic planning, technology adoption, and investment decisions. The vignette above illustrates the point: border operations can be deliberately designed not only to disrupt threats, but to generate system-level learning that drives lasting reform.

The experience of Jardena and Tin Can is not typical of how border challenges are handled. For many years, managing the border has been widely treated as an extension of TSOC, with both framed as a single national security priority. There is no doubt that this approach has delivered important enforcement outcomes, but it has also constrained how the border is understood, narrowing attention to criminal interdiction at the expense of its broader functions and strategic value. By viewing the border primarily through the lens of criminal commodities, Australia has underutilised its potential as an instrument of economic resilience, regulatory control, and geopolitical influence.

This crime-centric frame has also reinforced institutional siloes and, if it persists, will constrain Australia's ability to respond to emerging risks. Threats such as foreign interference, coercive trade practices, digital sabotage, and biosecurity can increasingly bypass traditional border enforcement models. When border policy is subordinated to a narrow law enforcement construct, these risks remain under-prioritised, fragmented, or addressed elsewhere in government without a coherent border strategy.

Reframing the border in national security planning

Recommendation 4

Review national security priorities to ensure maximum value is obtained from the border, ensuring coherent oversight, accountability, and strategic alignment across Australia's national priorities.

Additionally, the border increasingly intersects with adjacent government functions, from customs and immigration to cyber-security, from critical infrastructure to the regulation of data, and from health and biosecurity to finance. Reforms such as the *Security of Critical Infrastructure Act* (the *SOCI Act*),⁴⁵ the creation of the CISC⁴⁶ and new obligations relating to supply chain and cyber risk management, reflect a broader national shift toward the kind of integrated economic and security policy that this paper advocates. Yet border policy and governance remain largely siloed and absent from many of the integration efforts that are shaping Australia's national resilience agenda.

To initiate a necessary shift in perspective, this paper recommends that Australia recognises the border as a stand-alone national security and economic priority. This is not a call for a structural reorganisation, but deliberate signalling to ensure that border policy is treated as a strategic system in its own right, rather than a subordinate function of law enforcement or trade facilitation. Without this clarity at the highest level, border governance will remain disconnected from broader policy settings, limiting Australia's ability to anticipate, absorb, and respond to systemic risk.

To support and enable the evolution of border governance, consideration could also be given to leveraging Australia's international alliances, such as the Quadrilateral Security Dialogue, AUKUS, and Strategic Comprehensive Partnerships, to develop technologies, digital standards and data sharing mechanisms for trade and travel. The next section examines how such a shift in governance and ambition can be operationalised through federated systems, shared data architectures, and coordinated decision-making frameworks.

Federated learning systems: an architecture for modern border governance

“If we want things to stay as they are, things will have to change.”

Giuseppe Tomasi di Lampedusa, *The Leopard (Il Gattopardo)*, 1958.

This paradox now confronts border governance: preserving sovereignty, security, and public confidence requires deliberate modernisation. A rethink of Australia’s approach to border governance is fast becoming unavoidable. Technology is rapidly evolving and becoming embedded across global trade, travel, and logistics systems. Advanced analytics, AI, digital twins, and autonomous systems are changing the way risk is identified, decisions are made and operational interventions are applied across complex systems. These changes are moving faster than our current ability to govern their use.

Many of these technologies are already being deployed at borders by some countries, and the questions facing Australia are less about whether they will be used at the border, and more about when and how. The choices we make about system architecture, data sharing and governance will determine whether such tools enhance sovereignty, public trust, and resilience, or erode them. Delay is also potentially costly, allowing operating models, standards, and dependencies to be set elsewhere, diminishing Australia’s regional influence and strategic choices.

There is no settled answer as to how modern border systems should be configured, and a host of variables exist for individual countries to consider. Different architectures present different trade-offs between scale, control, agility, and trust, particularly in large-scale distributed systems where authority, data, and decision-making cannot be fully centralised.⁴⁷

Centralised data lakes offer powerful analytics but raise sovereignty, privacy, and security concerns.⁴⁸ Intelligence fusion centres can

foster coordination but are resource-intensive and difficult to scale.⁴⁹ SaaS (Software as a Service) solutions are widely available, making it easier to deploy AI across groups of stakeholders, but AI governance is still evolving, and concerns persist regarding data sovereignty, control, and assurance.⁵⁰

Nevertheless, viable options are emerging, and some are already operating in sectors facing similar complexity and risk, including healthcare, financial intelligence, and global trade analytics. This section examines one such option, federated learning systems, not as a panacea, but as a practical architecture designed to enable collaboration, scale, and insight without centralising control.

Federated learning is a machine learning approach in which models are trained across multiple decentralised datasets, without pooling the underlying data in a single location. Rather than sharing raw data, participants exchange model parameters and updates, allowing collaborative analytics while preserving privacy, legal control, and data sovereignty.⁵¹

Given the scale and complexity of border systems, machine learning is likely to play an increasing role in automated risk detection and decision support. The discussion of federated learning systems in this paper is not intended to advocate a single technical solution. Rather, it describes a distributed, privacy-preserving architecture that maintains sovereignty and legal control while making it feasible to deploy advanced analytics, including federated machine learning, across end-to-end trade and travel systems, improving detection, targeting precision, and system performance.

Federated learning systems are demonstrating tangible results in both commercial and government border-related settings. Their potential value lies in their ability to illuminate economic and logistics activity across borders, including global value chains – the functional integration and coordination of internationally dispersed activities required to bring a product or service from its initial conception to its final end use.⁵² This visibility spans production, ownership, trade, transport, compliance, and transformation of goods from true origin to end use.⁵³ Together, this provides a high-value operational lens and points the way towards what an expanded federated border system could achieve.

Mapping these and other data sets with customs and biosecurity data, in real time, and applying machine learning models across them, offers a pathway to producing highly valuable insights for operationally and strategically managing our border. Digital cargo screening images, customs declarations, geospatial, and other data from supply chain sensors, blockchain-derived risk scores, financial flows, and biosecurity alerts could all be encompassed. The focus would not just be on sharing insight, but also on early detection, prevention and disruption: where, how, and when to target intervention for maximum effect.

This section uses federated learning systems as shorthand for a distributed, privacy-preserving architecture with the functions and attributes needed to enable lawful collaboration and shared situational awareness at scale; highlighting the limits of agency-centric targeting models, which remain poorly equipped to integrate such data.

Limits of current targeting models

Australia's border systems have performed effectively in an era of relatively stable trade, predictable flows and transactional risk. As discussed earlier in this paper, the most consequential and contemporary threats no longer fit this profile, nor are they visible within today's agency-centric targeting models. They

sit within, and often between, financial, logistical, digital, and human systems that current targeting approaches were never designed to see.

Australia's border-targeting approach is designed to identify anomalies at the point of declaration, import, or arrival in an environment of relatively bounded threats and linear supply chains. This model has delivered strong results, but recent case studies expose its limits, particularly when confronting contemporary risks.

The Cabestro excise drawback scheme, which involved fraudulent claims for excise refunds and is estimated to have cost the Commonwealth more than A\$250 million,⁵⁴ was not detected through targeting systems. Instead, the scheme came to light only after diligent officers identified anomalous claims patterns, by which point hundreds of millions of dollars had been paid. The activity exploited regulatory and financial pathways, as well as container export logistics, a domain that is rarely screened, leaving such large-scale frauds largely invisible to conventional targeting.

By contrast, the trusted insider threats exposed through the AFP's covert Operation Ironside,⁵⁵ and subsequently addressed through Operation Jardena, revealed further significant border vulnerabilities. Insider access was being systematically used to bypass risk profiling and inspection regimes, exploit regulatory gaps, and neutralise detection capabilities that assumed good faith within accredited border environments.

In both cases the challenge was not effort or intent, but architecture. These significant risks, that in some ways mattered the most, lay beyond what a checkpoint-centric, agency-bounded targeting model is designed to see.

These cases also underscore how modern border risks are increasingly embedded within systems, or merge across systems, and cannot be managed through targeting models designed for isolated transactions and discrete jurisdictions.

From transactional targeting to systemic risk

These limitations have prompted experimentation with new approaches to targeting, extending beyond national borders and agency silos. Operation Tin Can demonstrated how like-minded customs administrations and industry partners could share risk signals and data, and coordinate targeting virtually, while retaining control over their data and legal authorities. Led by the ABF in partnership with the World Customs Organization, the six-week operation brought together 58 national customs authorities and several of the world's largest logistics providers to target insider-enabled narcotics concealment in containerised cargo. Reliance on centralised databases and uniform legal frameworks was minimised, and partners retained control of their data and operations while contributing risk signals to the shared intelligence picture. The power of distributed triage was to enable each partner to focus on the highest-value anomalies without swamping their systems.

Domestically, these insights also informed the evolution of the Targeting 2.0 concept within the ABF.⁵⁶ While a significant advance, those models still remain fundamentally agency-centric and insufficient for the cross-sector, cross-border risks now confronting the border system.

The implication is not just that existing targeting approaches are mismatched to the scale of the task, but that building the required data environment to address contemporary risks within a single agency would be inefficient and inappropriate. The utility of such an architecture is inherently cross-cutting, extending across economic security, national security, national resilience, crisis and emergency management, biosecurity, and law enforcement. It demands a different institutional design.

Importantly, many foundations for a federated system already exist, within legislative instruments such as the *SOCI Act*, collaborative models such as AUSTRAC's Fintel Alliance,⁵⁷ and multi-agency coordination hubs such as the CISC and National Emergency Management Agency. What's missing is a unifying framework to align data, mandates, and deci-

sion-making across the system as these foundations remain largely unconnected.

In a world that is becoming more fragmented and data-rich, no single agency can even remotely see the full picture, let alone ingest and analyse all relevant information. To derive insight and value at the scale of global trade and travel, as well as contemporary threats, algorithms may have to move to where data resides, whilst maintaining confidentiality and data sovereignty, and enabling distributed decision-making across trusted partners.

Digital architectures and federated learning systems

Managing risk at this scale requires a fundamentally different architecture from agency-centric systems. Today's reality is that our agencies and industry partners operate with distinct mandates and data regimes, and often act together, but without shared systems, protocols, or a common operating picture; despite some steps being taken to harmonise systems and improve interoperability.

Digital trade infrastructures have been explored for several years⁵⁸ and highlight why, and how, border agencies should be able to access and act on trusted supply chain data. The concept of data pipelines envisions secure, real-time streams of logistics information flowing between stakeholders, accelerating coordination and risk assessment. Whilst an improvement, pipelines of data in and of themselves will fail to deliver full advantage without some level of integration across portfolios and sectors.

Historically, governments have tended to meet complexity by centralising control, through portfolio restructuring, aggregating data, or building command hierarchies. The risk context today is defined by rapid change, data silos, and resource constraints. Abandoning command structures in operational agencies would be imprudent, but we will need to find ways to manage systemic risk with greater agility, precision, and coordination.

Federated systems offer one such approach. They are both a governance and technical model, which allow a broader group of partici-

Spotlight: federated learning in medical imaging

Federated learning is already used in healthcare to train AI models on sensitive medical images (CT scans, MRI, and X-Rays) across multiple hospitals without sharing patient data. Models are trained locally and only algorithmic updates are exchanged, preserving privacy, legal control, and data sovereignty.⁵⁹

Importantly this model operates within some of the most stringent regulatory and ethical frameworks in use today, while still delivering high-accuracy analytics across distributed datasets.⁶⁰ It demonstrates that sensitive, high-value data can be analysed at scale without centralisation.

The relevance to border governance lies in institutional design: data remains with its lawful owner, while insight is shared to support coordinated decision-making.

pants to access and analyse more data without pooling it, to collaborate more quickly, and to interpret and respond without duplicating effort or breaching confidentiality. Authority and data remain with participants, while shared alerts and analytical outputs support coordinated action.

While not a panacea, it could represent a step-change in capability. First, by unlocking the high value of data held by industry and international partners, and integrating it with domestic intelligence and regulatory holdings to generate actionable foresight, benefiting national agility and resilience. Second, when enabled by AI and machine learning, it would shrink the immense volume of movements and transactions across our border, improving regulatory efficiency and targeting precision. Third, it would reduce costly friction in legitimate supply chains, with less wasted inspection effort, better utilisation of scarce resources, and benefits flowing directly to exporters, importers, and the wider economy. Such an architecture could also support appropriately governed automation in risk detection and decision-making.

For Australia, the practical relevance of federated learning is clear. A cloud-native, layered architecture that integrates operational, regulatory, and industry data in real time alongside intelligence feeds would not just be a technology upgrade. It would represent a foundational element of national resilience, enabling earlier risk detection, more precise intervention, and enhanced coordination, while preserving data sovereignty and institutional authority.

Border modernisation will occur regardless, but it can be either reactive or deliberately designed. As industry embraces modern technologies, such as smart containers, blockchain-enabled logistics, and AI-driven automation, core government systems, including the ICS, risk lagging behind. The ICS was not designed to ingest or analyse the reservoirs of data that exist today, nor provide AI-enabled decision support or automated risk detection.

Without a unifying architecture, critical intelligence and valuable data will remain siloed or inaccessible, limiting the effectiveness of the border as both a strategic economic and national security asset.

From legacy systems to a National Border Visibility Platform

Recommendation 5

Design a blueprint for a National Border Visibility Platform as the digital backbone of cross-portfolio border governance, enabling shared situational awareness, policy implementation and performance monitoring, coordinated prioritisation, and timely operational decision-making. Working under the leadership of the Expert Advisory Board, and building on the Simplified Trade System reform, this platform should incrementally replace the Integrated Cargo System and lawfully share data across government and industry.

Taken together, the challenges outlined in this section cannot be addressed through incremental upgrades to existing systems. Designing a blueprint for a National Border Visibility Platform is recommended as a means of creating a digital backbone for cross-border governance.

Under the stewardship of the National Border Coordination Committee (Section 5.3), informed by expert advice from the Expert Advisory Board, this blueprint could build on work already under way as part of the STS reform and guide a phased transition from legacy systems, including the progressive retirement of the ICS, rather than continuing to extend systems that were never designed for today's data, risk, and operating environment.

Meeting these requirements points to an architecture that is not based on centralised control, but on coordinated and distributed visibility. The various layers of a Border Visibility Platform could operate interdependently, connecting distributed, trusted partners through shared risk signals, aligned processes, and interoperable tools, supported by AI-enabled analytics and transparent rules-based decision engines.

Layer 1: data access

A foundational layer is necessary to enable controlled access to high-value data sources, while sensitive government and commercial data remains with its owners. The aim is to ensure the right datasets, whether domestic, international, or commercial, can be queried in near real-time through agreed data-sharing protocols, secure gateways, and governance arrangements that protect sovereignty and privacy. For example, a suspicious shipment flagged by overseas customs could trigger an automated query of Australian datasets, enabling a risk assessment to occur before the goods are loaded and reducing the likelihood of compliance or security breaches.

Layer 2: data integration and analytics

With Layer 1 gathering and protecting high-fidelity inputs, it is necessary to create a layer to make them usable by securely combining relevant elements from different sources into

a shared analytical frame, applied through federated models and rules engines, without moving all the raw data. This could entail comparing a flagged container manifest with customs declarations, trade-finance records, or other industry data. The result is a context-rich view of the movement, ownership, and risk profile of goods, supply chains, or travellers, enabling far more precise targeting than with today's generic rules-based profiles.

Layer 3: decision support and action

With the picture assembled, it becomes necessary to translate it into action, and this is where the proposed National Visibility Platform comes into play. Signals become operational decisions, from automated alerts to coordinated multi-agency responses. By integrating into existing command centres and workflows, agencies and their officers can act with the same intelligence picture. This layer accelerates triage, reduces the risk of duplication or inaction, and directs scarce resources to the highest-risk consignments or travellers, while letting low-risk flows move unimpeded.

Layer 4: assurance and governance

It will be essential to maintain public trust by demonstrating adherence to legislative standards, such as the Australian Privacy Principles,⁶¹ particularly where the use of AI is concerned. Clear legal frameworks, auditability, and transparent governance is essential. This layer provides assurance across the system by monitoring system performance and compliance, for example by tracking strike rates, disruption outcomes, AI bias, and any breaches of privacy, confidentiality, or cyber security, enabling continuous improvement.

Together, these layers form a functional architecture capable of supporting border governance at scale. Realising such a system depends not only on technology, but on regulatory, institutional, and investment mechanisms to enable it, which are addressed in the next section.

From architecture to delivery

“When we talk about the Fourth Industrial Revolution, it’s not primarily about technologies themselves.”

Klaus Schwab (2016), Founder and Executive Chairman, World Economic Forum.

If the Fourth Industrial Revolution is ultimately about transforming systems rather than deploying technology, then modernising the border is best approached as being institutional reform as much as technological reform. While Section 4 of this paper sketches out the architecture of a modern, data-enabled border, implementing it would be a far more demanding task and enliven several areas of legislation and regulation, including Australia’s Privacy Principles, the Protective Security Policy Framework,⁶² Hosting Certification Framework⁶³ and the *SOCI Act*. A lot of legal and policy groundwork would be necessary.

Managing Australia’s international border is constitutionally and legislatively a Commonwealth responsibility. Its effective operation, however, depends on coordination with state and territory governments and agencies, particularly in port operations, policing, public health, and emergency management. The COVID-19 pandemic, and the *Ruby Princess* incident in particular, highlight how quickly gaps in shared assumptions can translate into operational consequences at the border. Border modernisation therefore requires a whole-of-system approach, incorporating interoperability and governance, including where the primary legislative and policy levers remain federal.

Legal and policy foundations for a trusted digital border

Recommendation 6

Review border-related legislative and policy frameworks that underpin the design of digital systems to preserve data sovereignty, protect privacy, uphold public trust, and enable system-wide data-sharing, interoperability, and coordinated decision-making.

It is therefore recommended that border-related legislative and policy frameworks be reviewed to establish principles and guardrails that enable data sharing and the use of AI. This work should be directed towards enabling the outcomes that this paper envisages, maintaining social licence and public trust, and informing the design and implementation of a future digital border architecture.

Given the strain on many portfolio budgets and resources, the full costs and benefits of implementing the recommendations in this paper should be explicitly assessed. Without the sustained support of government, reform at the scale proposed here is unlikely to succeed; alternative funding and investment approaches should therefore be considered alongside policy and regulatory reform.

Hidden costs

Australia’s border agencies deliver impressive operational outcomes each year, seizing large volumes of illicit drugs, tobacco, and other contraband, and in keeping our airports moving. However, these successes mask a set of structural inefficiencies and hidden costs that are increasingly difficult to sustain.

As outlined in Section 2, Australia’s border management approach relies on risk-based targeting to prioritise physical inspection and interdiction. In practice, this model carries inherent structural constraints that limit its scalability and the assurance it can provide across complex and fast-moving supply chains.

At the same time, Australia’s border operating model is increasingly misaligned with modern port logistics. As industry shifts towards inter-modal hubs and inland container terminals⁶⁴ to manage growing trade volumes and free up wharf space, inspection approaches centred

on waterfront locations become slower, more expensive, and less effective.

This shift also presents a rare opportunity to re-think the end-to-end model for cargo screening and risk assessment. Co-design with industry could enable much broader screening coverage and more precise targeting, without adding friction for compliant traders.

Opportunities also exist upstream with overseas partners. Some customs administrations already exchange X-ray images and risk information on outbound cargo, enabling earlier intervention before goods are loaded for export. Australia has several Comprehensive Strategic Partnerships and trade agreements that could be used to support similar arrangements, strengthening prevention while reducing downstream costs.

Spotlight: cross-border cooperation

Brazil and the Netherlands have established a cooperative model in which outbound containers are screened using X-ray technology, with digital imagery and associated risk information shared prior to arrival. In this model, upstream data enables narcotics concealment to be targeted earlier in the supply chain, reduces reliance on inspection at congested arrival ports, and allows resources to be focused on the highest risk consignments.⁶⁵ Such arrangements demonstrate how shared visibility can improve detection rates and reduce friction and cost.

The economic and social implications of such structural limits are also significant. Criminal groups continue to traffic large volumes of illicit drugs and tobacco across Australia's border, and pocket billions of dollars in profit. Official wastewater analysis indicates that more than 22 tonnes of major illicit drugs were consumed in Australia between August 2023 and August 2024, a 34 per cent increase on the previous year.⁶⁶ The growth in illicit drug and tobacco markets points to sustained leakage across the border, despite ongoing enforcement successes and upstream cooperation with international partners.

The costs extend far beyond agency budgets. Illicit narcotics and tobacco impose substantial downstream burdens on the public purse, across health, social services and the criminal justice system. They are also seriously undermining public health and taxation policy objectives. Where leakage at the border remains high, downstream enforcement and regulatory agencies also become stretched and find it difficult to achieve their intended effect. Prevention and deterrence cannot be delivered by domestic enforcement alone, and without improvements in border screening, targeting, and early intervention, key policy levers will continue to operate with diminished effect.

Strengthening Australia's targeting and screening capability would reduce risk, reinforce key policy levers, and materially limit the direct and indirect impacts of illicit cross-border activity, including the health and social harms associated with narcotics and nicotine products, and the losses from duty evasion and revenue fraud.

Beyond detecting contraband, Australia's border management functions include international travel and migration, biosecurity, customs, financial flows, and the protection of intellectual property across both physical and digital supply chains. To manage complexity, border policy has often been organised around discrete functional priorities, such as illicit tobacco enforcement, which can obscure and diminish this broader role.

This helps explain why many border sub-systems remain fragmented. Across multiple locations, border agencies operate side-by-side, with officers working in close proximity and using similar processes and technologies, but relying on separate platforms, suppliers, and data environments that are unable to connect.

With trade volumes and threat complexity projected to grow, Australia will struggle to

keep pace without better integration across portfolios and a more scalable model of risk detection and intervention. This requires a shift in how border risk is detected, shared and acted upon.

- Traditional targeting and post-incident response → automated risk detection and precision intervention.
- Siloed intelligence and data → real-time federated learning and coordinated risk management.
- Static rules-based processing → regulatory grade AI, augmentation, and dynamic decision-making.

These shifts can be pursued incrementally, building on several existing reform and collaborative initiatives, including the STS and elements of the *Aviation White Paper*.

Australia also has legislative mechanisms to enable this approach, including a regulatory sandbox within the *Customs Act*.⁶ This provides a controlled environment to test new data-sharing arrangements, analytical tools, and operating models, surfacing regulatory friction early and helping to identify where regulatory-grade AI is required for risk management and decision support.

Regulatory-grade artificial intelligence

Key portfolios and agencies performing border, economic, and regulatory functions operate under distinct mandates and frameworks. This creates friction across the border system, particularly for industry, by slowing decisions, creating blind spots, duplicating effort and limiting visibility across trade and travel movements.

Looking ahead, regulatory alignment across the border system is not a matter of policy consensus alone and increasingly about technical and data integration. Regulatory-grade AI is emerging in healthcare and refers to AI systems that meet formal requirements for safety, transparency and accountability, consistent with frameworks such as the EU's Artificial Intelligence Act.⁶⁸ This requires AI systems to be accurate, explainable, privacy-preserving, reliable under real-world operational conditions, and subject to independent assessment before deployment.

If AI systems that meet strict data privacy and security standards are feasible, there is a pathway to regulatory alignment and interoperability at the border without centralisation. Portfolios and agencies can translate complex rules from across regimes into machine-readable logic, allowing faster decision support, shared risk ratings, and automated compliance checks. In practical terms, regulatory-grade AI enables three concrete shifts.

- **Cross-domain risk orchestration** – aligning trade, biosecurity, health, and security risk settings within a common analytical framework.
- **Dynamic rule interpretation** – updating prioritisation and triage as regulatory requirements change, without manual intervention.
- **Embedded compliance logic** – converting agency rules and thresholds into machine-readable workflows, automating low-risk clearances, reducing friction for legitimate flows and flagging high-risk anomalies.

Many legislative foundations for risk-based information sharing and assurance already exist, for example within the *SOCI Act 2018*,⁶⁹ *Customs Act 1901*,⁷⁰ *Biosecurity Act 2015*,⁷¹ *Australian Border Force Act 2015*,⁷² and the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*.⁷³

Interoperability, law and governance

It would be reasonable to argue that border management and reform should remain portfolio-based, given legal boundaries, operational accountabilities and budget constraints. These concerns are legitimate; portfolio accountability and statutory responsibility matter, particularly in high-risk environments. However, the trendline in strategic competition, grey zone activity and supply chain exploitation means that fragmentation itself now creates systemic risk, limiting visibility, slowing coordination, and allowing vulnerabilities to persist. The intention behind this paper is not to centralise border functions within a single portfolio, but to strengthen interoperability, coherence, and shared assurance across government while preserving institutional independence.

A primary constraint in Australia's border environment is the absence of a governance model capable of aligning mandates, data, and decision-making across the system. While the legislative arrangements are largely in place, they are applied through organisational structures that inhibit interoperability, dilute accountability, and constrain coordination. Addressing this requires a more cross-cutting governance model that treats public trust, interoperability and legal coherence as foundational enablers of system-wide performance and establishes a mechanism to align priorities and investment across portfolios.

Public trust and social licence for border modernisation

Recommendation 7

Conduct a national program of public research to strengthen public confidence and legitimacy for border modernisation by assessing community perceptions, expectations, and trust thresholds concerning the use of data, digital infrastructure, and AI-enabled decision support.

Public trust in institutions is not a given and is constantly being shaped by the lived experience of Australians in a period of heightened uncertainty. Global turmoil, crime, cyber-crime, and illicit markets all contribute to this environment and are amplified through social media. At the same time, visible social harms including addiction, family and domestic violence, youth crime, road trauma, and preventable deaths are directly influencing perceptions about community safety and household wellbeing.

Increasing the use of data, digital infrastructure and AI-enabled decision support at the border inevitably raises legitimate questions about privacy and accountability. More importantly, it raises a practical question for the community: are these systems actually reducing harm? Legislative safeguards are essential, but without a clear understanding of community expectations and trust thresholds, border modernisation risks becoming politicised or contested, even when the operational case is strong.

Australia conducts rigorous public research and polling on immigration, social cohe-

sion and trust in government. However, there appears to be no comparable national research focussed on community support for border modernisation, particularly the trade-offs Australians are willing to accept between faster facilitation and maintaining strong border security when shared data, digital infrastructure, and AI-enabled decision support are proposed. To address this gap, it is recommended that a national research program be conducted to strengthen public confidence and legitimacy for border modernisation, and to understand community expectations, perceptions and trust about the use of data, digital infrastructure and AI-enabled decision support at the border.

Interoperability by design

Australia's border operations span many platforms, agencies, and mandates. Without improving interoperability across data structures, systems, and legal authorities, it is unlikely that effective coordination can occur. Looking ahead, border operations will increasingly require digital systems that connect portfolios, sectors, agencies, and data coherently.

Such digital architectures would include tools to organise and harmonise data, apply common definitions, and have standard connections (APIs). This aligns with the concept of federated systems and trusted AI discussed earlier. These architectures would translate complex rules into usable formats, helping to speed up decision-making, share risk ratings, and support coordinated action in real time.

Legal coherence

Digital architectures cannot function without a lawful basis for sharing information across them. In this regard, Australia's legislative framework appears to be in relatively good shape. There may still be gaps in legal authorities, along with an overly cautious application of secrecy provisions and divergent agency interpretations about them. This can constrain collaboration and diminish the public value extracted from the border.

Before constructing new legal authorities, it would be sensible to formalise existing portfolio-level mechanisms for lawful, auditable

data sharing across the system. By embedding protocols such as inter-agency MOUs, model clauses, and regulatory sandboxes, institutional independence can be preserved while still enabling more effective collaboration.

Institutional alignment and cross-portfolio governance

Recommendation 8

Establish a National Border Coordination Committee, bringing together the heads of key departments and agencies (drawing on the Expert Advisory Board as required) to shape standards, prioritise risk, and oversee the implementation of a strengthened federated border.

Australia's border system lacks a standing governance mechanism with the authority and remit to align priorities, standards, and investment across portfolios. Governance is dispersed across various committees, bilateral arrangements, and program-specific initiatives, which can inhibit coordination and make sustained reform difficult.

A standing governance mechanism that spans portfolios would provide the necessary coherence. Drawing on the model of New Zealand's Border Executive Board, established under the *NZ Public Service Act 2020*,⁷⁴ Australia could establish a National Border Coordination Committee.

As a senior level, durable centre of gravity, it would help provide the authority needed to cut through duplication, address cross-system constraints, and sustain momentum across election and budget cycles, while strengthening accountability and public trust.

Funding and sustainability

The term 'asset' is deliberately used in this paper to signal that the border requires sustained investment if we are to retain, or increase, its strategic value. The current fund-

ing model relies on annual portfolio budgets, which makes it difficult for an incumbent government to anticipate or prioritise longer term capability requirements, and therefore difficult to develop the border and its underlying systems.

For the border to become a strategic economic and national security asset, from which optimal public value is acquired, where costs are minimised and investments phased, a funding approach that dovetails with annual budgets, supports co-design, and unlocks new funding mechanisms would be more likely to succeed. This may require the consideration of new funding pathways.

Border-generated revenue

Customs duties, GST on imports, excise-equivalent collections, import processing charges, and proceeds from enforcement actions, are all examples of how the border generates value. A strategic feedback loop, where a proportion of future revenue-generation is linked with infrastructure renewal, could be used to partially insulate critical elements of modernisation from short-term budget pressures and align investment with the national interest.

Public-private coinvestment

Operators in freight, ports, and logistics have a clear interest in creating an agile and resilient border with minimal friction. Industry contributions, such as through aviation security and port sector levies, could be more clearly tied to structured investments; providing a line of sight between revenue generated at the border and its re-investment.

Australia's New and Redeveloping International Ports process⁷⁵ has been earmarked for review by the *Aviation White Paper*⁸ and already requires port operators to finance elements of border infrastructure at their facilities, providing a practical precedent for future co-design and co-funding of modernisation.

In 2024, an airport operator purchased new smart gate kiosks for the ABF to operate and maintain,⁷⁶ indicating a potential blueprint for structured public-private capability partnerships across Australia's ports and borders.

Sovereign capability investment pathways

Recommendation 9

Establish a National Border Investment Framework to align approvals, investment decisions, and the national interest, supporting the transition from episodic risk treatment to embedded system-wide assurance. The framework should drive prioritisation based on public value and national security outcomes, under the oversight of the National Border Coordination Committee.

The Future Made in Australia Act 2024⁷⁷ establishes a National Interest Framework, including an economic resilience and security stream, to guide significant public investment that unlocks private investment at scale. That logic could be applied to border modernisation as sovereign-enabling infrastructure for economic resilience and security. National digital resilience programs could also potentially be expanded to encompass key elements of border modernisation, elevating the border from a transactional enforcement function to a strategic asset within Australia's sovereign capability ecosystem.

To institutionalise long-term investment, the establishment of a National Border Investment Framework is recommended: a standing investment mechanism governed by the National Border Coordination Committee, with structured participation from industry partners. The intent is not necessarily to create a new funding line, but to establish a mechanism to align, sequence and assure existing investments against national outcomes, including through co-investment models where appropriate. This framework would support the phased development of core capabilities, including data integration, digital and physical infrastructure, regulatory-grade AI systems, cyber resilience, and cross-agency platforms.

This would be forward leaning, but not without precedent. Comparable Commonwealth funding mechanisms, such as the Modern Manufacturing Initiative⁷⁸ and Australia's Medical Research Future Fund,⁷⁹ demonstrate how targeted public investment can be used to steer long-term capability uplift in the national interest. Implementation could be phased, with initial funding drawn from existing programs and progressively scaled over time. Ultimately, investing in our border is a commitment to Australia's renewal, requiring not just capital, but a shift in our planning horizons, accountability mechanisms, and the way we define the border's value to national prosperity and security.

Conclusion

“Great powers have begun using economic integration as weapons, tariffs as leverage, financial infrastructure as coercion, supply chains as vulnerabilities to be exploited.”

Canadian Prime Minister Mark Carney, remarks at World Economic Forum, Davos, 2026.

Australia finds itself in precisely the circumstances Carney describes, and many of the assumptions that underpin our approach to border management (seamless trade and travel, globalisation, manageable risk) no longer hold true. Any credible vision for Australia's border in the coming years should be grounded in strategic foresight, deeper coordination, and a clearer understanding of how the flows of people, goods, data, and capital shape national security and economic resilience.

This paper has argued that Australia's border is now a point of convergence between economic resilience, geopolitical leverage and the defence of sovereignty, while being simultaneously exposed to sophisticated and systemic threats. Managing the border through static, siloed, operating models in this environment not only reduces efficiency, but also diminishes Australia's strategic agility and underutilises one of the nation's powerful instruments of economic and regulatory statecraft.

To meet the challenges of a multipolar, digitally entangled world, Australia would be better positioned by evolving its border from a series of checkpoints into a cohesive, federated system enabled by data and AI, underpinned by robust legal and governance frameworks, and designed for collaboration across government, industry, and international partners. This is foundational to safeguarding our sovereignty, strengthening our security, enabling legitimate trade and travel, and sustaining Australia's influence in the region.

Without clear government sponsorship, enduring delivery mechanisms and alignment with broader economic and national security strategies, the Australian border risks remaining an underleveraged asset of national significance that is caught between sound intentions and fragmented implementation. Public understanding of the border is often shaped only by its most visible touchpoints, such as a smart gate, obscuring the scale and strategic importance of the system beneath it. At the same time, tolerance for friction at the border remains. Australians expect their border to be both protective and seamless; an expectation that cannot be met through manual processes or disconnected systems.

The window for creating a resilient, agile, and future-ready border is narrowing. Australia can choose to have a border with strategic clarity, digital capability, and institutional purpose, or risk being overtaken by events, as occurred during the COVID-19 pandemic.

With the Brisbane 2032 Olympic Games quickly approaching, the ambition should be clear: a border that is integrated, adaptive, and trusted, that reflects Australia's values while meeting the demands of a more contested world. The opportunity remains open but only for a limited time.

References

1. Geoscience Australia (2025) *Oceans and Seas*. Available at: <https://www.ga.gov.au/scientific-topics/national-location-information/dimensions/oceans-and-seas> (Accessed: 9 January 2026).
2. Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts (2025) Designated international airports in Australia and Australian seaports dataset. Available at: <https://www.infrastructure.gov.au/infrastructure-transport-vehicles/aviation/international-aviation/multilateral-forums/icao/international-airports> (Accessed: 9 January 2026).
3. Australian Border Force (2025) Ports of entry. Available at: <https://www.abf.gov.au/entering-and-leaving-australia/entering-and-leaving-by-sea/ports-of-entry> (Accessed: 9 January 2026).
4. Outram, M (2024) National Press Club Address, Australian Border Force, 16 October 2024. Available at: <https://www.abf.gov.au/newsroom-subsite/Pages/National-Press-Club-of-Australia-address.aspx> (Accessed: 6 August 2025).
5. Froman, MBG (2025) 'After the Trade War: Remaking Rules From the Ruins of the Rules-Based System', Foreign Affairs, 11 August 2025.
6. HM Government (2023) Integrated Review Refresh 2023: Responding to a more contested and volatile world, Cabinet Office, UK Government, 13 March 2023. Available at: <https://www.gov.uk/government/publications/integrated-review-refresh-2023-responding-to-a-more-contested-and-volatile-world/integrated-review-refresh-2023-responding-to-a-more-contested-and-volatile-world> (Accessed: 9 January 2026).
7. Government of Japan (2022) National Security Strategy, Cabinet Office, 16 December 2022. Available at: <https://www.cas.go.jp/jp/siryoku/221216anzenhoshou/nss-e.pdf> (Accessed: 9 January 2026).
8. Department of Infrastructure, Transport, Regional Development, Communications and the Arts (2024) Aviation White Paper – Towards 2050, Sections 1, 4, 8 and 12.2, [online]. Released 26 August 2024. Available at: <https://www.infrastructure.gov.au/infrastructure-transport-vehicles/aviation/aviation-white-paper> (Accessed: 9 January 2026).
9. Australian Government, Department of Foreign Affairs and Trade (2025) *Russia sanctions framework*, DFAT, Canberra. Available at: <https://www.dfat.gov.au/international-relations/security/sanctions/sanctions-regimes/russia-sanctions-framework> (Accessed: January 2026).
10. Centre for Research on Energy and Clean Air (2024) *Russia's Fossil Fuel Exports: Revenues, Destinations and Sanctions Implications*. Helsinki: CREA. Available at: <https://energyandcleanair.org> (Accessed: 1 January 2026).
11. Centre for Research on Energy and Clean Air (2025), *Tracking Russian Crude and Refined Product Exports Through Third Countries*. Helsinki: CREA. Available at: <https://energyandcleanair.org> (Accessed: 1 January 2026).
12. Commonwealth of Australia (2024–25) *Senate Estimates: Foreign Affairs, Defence and Trade Legislation Committee; Legal and Constitutional Affairs Legislation Committee – Evidence*. Canberra: Parliament of Australia. (Hansard transcripts, questioning of Department of Home Affairs and Australian Border Force officials on sanctions enforcement and Russian oil imports, November 2024 and May/November 2025). Available at: https://www.aph.gov.au/Parliamentary_Business/Hansard (Accessed: 5 January 2026 via committee transcripts).
13. Australian Trade and Investment Commission (Austrade) (n.d.) *Simplified Trade System*, Austrade. Available at: <https://www.austrade.gov.au/en/how-we-can-help-you/programs-and-services/simplified-trade-system> (Accessed: 9 January 2026).
14. Uren, D & Australian Strategic Policy Institute (2024) 'The trade routes vital to Australia's economic security'. Australian Strategic Policy Institute, Barton, ACT. [online] Available at: <https://www.aspi.org.au/report/trade-routes-vital-australias-economic-security> (Accessed: 10 January 2026).
15. Farrell, H and Newman, AL (2019) 'Weaponized Interdependence: How Global Economic Networks Shape State Coercion', *International Security*, 44(1), pp. 42–79. doi: 10.1162/ISEC_a_00351.
16. Azad, TM (2023) 'Understanding the gray zone', *Journal of Strategic Security*, vol. 16. P.87. doi:10.1177/00438200221141101.
17. Australian Bureau of Infrastructure, Transport and Regional Economics (2023) *Australian Sea Freight 2022–23*, Australian Government. Available at: <https://www.bitre.gov.au/publications/2023/australian-infrastructure-and-transport-statistics-yearbook-2023/shipping> (Accessed: 10 January 2026).
18. Australian Bureau of Statistics (2023) *International Trade: Supplementary Information, Calendar Year 2022*, Australian Government. Available at: <https://www.abs.gov.au/statistics/economy/international-trade/international-trade-supplementary-information-calendar-year/2022> (Accessed: 6 August 2025).

19. Muradov, K, (2022) *Trade costs and borders in global value chains*. OECD Trade Policy Paper No. 261. Paris: OECD Publishing. Available at: <https://doi.org/10.1787/2e5f7ecd-en> (Accessed: 6 August 2025).
20. Australian Border Force (2024) 'Australian Trusted Trader'. Available at: <https://www.abf.gov.au/about-us/what-we-do/trustedtrader>.
21. McGregor, R (2022) *Chinese coercion, Australian resilience*. Sydney: Lowy Institute for International Policy. Available at: <https://www.lowyinstitute.org/publications/chinese-coercion-australian-resilience> (Accessed: 10 January 2026).
22. HM Government (2020) *The 2025 UK Border Strategy*. Cabinet Office, December. Available at: <https://www.gov.uk/government/publications/2025-uk-border-strategy> (Accessed: 6 August 2025).
23. Immigration and Checkpoints Authority (2024) *Automated Clearance Initiative and Biometric Border Strategy*, Singapore Ministry of Home Affairs, 30 April. Available at: <https://www.ica.gov.sg/news-and-publications/newsroom/media-release/redefining-border-clearance-and-service-delivery> (Accessed: 6 August 2025).
24. Executive Office of the President (2021) *Executive Order 14017: America's Supply Chains*, Presidential Documents, issued 24 February. Available at: <https://www.govinfo.gov/content/pkg/DCPD-202100163/pdf/DCPD-202100163.pdf> (Accessed: 6 August 2025).
25. Government of Japan (2022) *National Security Strategy of Japan*, Cabinet Office, December. Available at: <https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-e.pdf> (Accessed: 6 August 2025).
26. Government of Japan (2022), *Outline of the Economic Security Promotion Act* (tentative English translation), Ministry of Justice. Available at: <https://www.japaneselawtranslation.go.jp/outline/75/905R403.pdf>. (Accessed: 4 August 2025).
27. European Commission & High Representative (2023), Joint Communication on European Economic Security Strategy (JOIN(2023)20), European Commission, published 20 June. Available at: https://ec.europa.eu/commission/press-corner/api/files/document/print/en/ip_23_3358/IP_23_3358_EN.pdf (Accessed: 6 August 2025).
28. Office of National Security / Ministry of Foreign Affairs (2023), *The Yoon Suk-yeol Administration's National Security Strategy: Global Pivotal State for Freedom, Peace and Prosperity*, issued 7 June 2023, English version published 8 June. Available at: https://www.mofa.go.kr/eng/brd/m_25772/view.do?page=1&seq=16 (Accessed: 4 August 2025).
29. HM Government (2023), *National Security and Investment Act 2021 – Annual Report 2023*, Department for Business and Trade, July. Available at: <https://www.gov.uk/government/publications/national-security-and-investment-act-2021-annual-report-2023> (Accessed: 7 January 2026).
30. Executive Office of the President (2022), *National Security Strategy of the United States of America*, October 12, 2022, Washington, DC. Available at Internet Archive: <https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.pdf> (Accessed: 6 August 2025).
31. Australian Strategic Policy Institute (2025), 'Mapping a decade's worth of hybrid threats targeting Australia', *The Strategist*, 7 May. Available at: <https://www.aspistrategist.org.au/mapping-a-decades-worth-of-hybrid-threats-targeting-australia> (Accessed: 6 August 2025).
32. Pedrozo, R (2021) 'China's Container Missile Deployments Could Violate the Law of Naval Warfare', *International Law Studies*, Vol. 97, pp. 1160–1170.
33. U.S. Army TRADOC (n.d.) Club-K Russian Container Short-Range Anti-Ship Cruise Missile. ODIN (Operational Detachment Intelligence Network) – Weapons & Equipment Guide. Available at: <https://odin.tradoc.army.mil/WEG/Asset/6c36b78eefbf3f88e093e2de99da354> (Accessed: 10 January 2026).
34. International Monetary Fund (IMF) (2025), *CryptoAssets Monitor: Q2 2025*, IMF Monetary and Capital Markets Department, 23 May, report, p. 2 (market update). Available at: <https://www.imfconnect.org/content/dam/imf/News%20and%20Generic%20Content/GMM/Special%20Features/Crypto%20Assets%20Monitor.pdf> (Accessed: 6 January 2026).
35. United Nations Office on Drugs and Crime (n.d.), *Money laundering overview*, UNODC. Available at: <https://www.unodc.org/unodc/en/money-laundering/overview.html> (Accessed: 8 August 2025).
36. Office of the Illicit Tobacco and E-Cigarette Commissioner (2025), *Illicit Tobacco and E-Cigarette Commissioner Report 2024-25*. Australian Government, Canberra. Available at: https://www.itec.gov.au/sites/default/files/2025-12/ITEC_Commissioner-Report_2024-25.pdf (Accessed: 6 January 2026).
37. Financial Action Task Force (FATF) 2025, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*, FATF. Available at: <https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2025-Targeted-Update-VA-VASPs.pdf.coredownload.pdf> (Accessed: 5 January 2026).
38. Australian National Audit Office (2020), *Container Examination Facilities*, Audit Report No. 16 of 2004–05, ANAO, Canberra, p.11. Available at: https://www.anao.gov.au/sites/default/files/ANAO_Report_2004-2005_16.pdf (Accessed: 6 January 2026).

39. Bureau of Infrastructure and Transport Research Economics (2023), Australian sea freight 2000–01 to 2022–23, BITRE Statistical Report, Australian Government, Canberra. Available at: https://www.bitre.gov.au/statistics/maritime/australian_sea_freight (Accessed: 5 January 2026).
40. Special Commission of Inquiry into the Ruby Princess (2020), Report of the Special Commission of Inquiry into the Ruby Princess. New South Wales Government. Available at: <https://www.nsw.gov.au/sites/default/files/2023-07/Report-of-the-Special-Commission-of-Inquiry-into-the-Ruby-Princess.pdf> (Accessed: 17 August 2025).
41. European Union (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L119, pp. 1–88.
42. Simplified Trade System Taskforce (2023), *Simplifying Trade System: Progress and Opportunities*, Simplified Trade System Implementation Task Force, Canberra, p. 2. Available at: <https://www.austrade.gov.au/en/news-and-analysis/publications-and-reports/sts-progress-and-opportunities-august-2023> (Accessed: 8 January 2026)
43. Parliament of Australia (2023), Estimates Committee Hansard, 23 May 2023, discussion of Operation Jardena and its establishment, Parliament of Australia, Canberra. Available at: https://www.aph.gov.au/Parliamentary_Business/Hansard/Hansard_Display?bid=committees/estimate/26893&sid=0003 (Accessed: 8 January 2026).
44. World Customs Organization (2023) *98 tonnes of cocaine seized in WCO-UNODC Operation Tin Can tackling organized crime and insider threats exploiting the supply chain*, 4 April. Available at: <https://www.wcoomd.org/en/media/news-room/2023/april/98-tonnes-of-cocaine-seized-in-wco-unodc-operation-tin-can-tackling-organized-crime.aspx> (Accessed: 8 January 2026).
45. Commonwealth of Australia (2018), *Security of Critical Infrastructure Act 2018*.
46. Cyber and Infrastructure Security Centre (2024), 'About the Cyber and Infrastructure Security Centre'. Available at: <https://www.cisc.gov.au/about-us> [Accessed: 22 August 2025]
47. Yau, SS, Yao, Y, & Buduru, AB (2014), An adaptable distributed trust management framework for large-scale secure service-based systems. *Computing*, 96, 925–949.
48. Joodala, A. (2025) 'Secure data lake architectures for public sector analytics', *International Journal for Multidisciplinary Research*, 7(4), July–August, pp. 1–14.
49. United States Government Accountability Office (2014), *Information Sharing: DHS is Assessing Fusion Center Capabilities and Results, but Needs to More Accurately Account for Federal Funding Provided to Centers*, GAO-15-155, Washington, DC: GAO. Available at: <http://www.gao.gov> (Accessed: 7 January 2026)
50. *Computer Weekly* (2025), 'Business leaders raise concerns over public cloud data sovereignty', 23 October. Available at: <https://www.computerweekly.com/news/366633439/Business-leaders-raise-concerns-over-public-cloud-data-sovereignty> (Accessed: 7 January 2026).
51. Kairouz, P, McMahan, HB, Avenet, et al. (2021) 'Advances and Open Problems in Federated Learning', *Foundations and Trends® in Machine Learning*, 14(1–2), pp. 1–210. Available at: <https://arxiv.org/pdf/1912.04977> (Accessed: 11 January 2026).
52. Gereffi, G, Humphrey, J and Sturgeon, T (2005) 'The governance of global value chains', *Review of International Political Economy*, 12(1), pp. 78–104
53. Bersin, A, Swartz, P and Karlsson, L (2025) 'Managing Supply and Value Chains in a New Era of Global Trade: The Promise of Federated Learning', *World Customs Journal*, 19(1), pp. 100–141.
54. Australian Federal Police (2025), *Australian Federal Police Annual Report 2024–25*, Australian Federal Police, Canberra, p. 21 (Operation Cabestro excise evasion estimated loss). Available at: <https://www.afp.gov.au/sites/default/files/2025-10/AFPAnnualReport2024-25.pdf> (Accessed: 7 January 2026)
55. Australian Federal Police (2024), Operation Ironside, Australian Federal Police, 8 August. Available at: <https://www.afp.gov.au/about-us/history/unique-stories/operation-ironside> (Accessed: 8 January 2026).
56. Australian Border Force (ABF) (2024), Navigating Today's Volatility, Uncertainty, Complexity and Ambiguity Environment – The Australian Border Force Experience, speech by Michael Outram APM, Commissioner and Comptroller-General of Customs, Leaders in Crisis Management Forum, 5 April, Australian Government. Available at: <https://www.abf.gov.au/newsroom-subsite/Pages/ABF-Commissioner-Michael-Outram-05-04-2024.aspx> (Accessed: 8 January 2026).
57. AUSTRAC (2025), AUSTRAC expands Fintel Alliance to strengthen fight against financial crime, AUSTRAC. Available at: <https://www.austrac.gov.au/austrac-expands-fintel-alliance-strengthen-fight-against-financial-crime>. (Accessed: 23 August 2025).

58. Rukanova, B, Henriksen, HZ, Henningsson, S & Tan, Y-H (2017), 'The Anatomy of Digital Trade Infrastructures', in Johansson, B, Møller, C, Chaudhuri, A & Sudzina, F (eds), *Perspectives in Business Informatics Research: Proceedings of the 16th International Conference on Business Informatics Research (BIR 2017)*, Lecture Notes in Business Information Processing, vol. 295, Springer, Cham, pp. 184–198.
59. Sheller, MJ, Edwards, B, Reina, GA *et al.* (2020), *Federated learning in medicine: facilitating multi-institutional collaborations without sharing patient data*. Scientific Reports, 10, 12598. Available at: <https://doi.org/10.1038/s41598-020-69250-1> (Accessed: 8 January 2026).
60. Schmidt, J, Schutte, NM, Buttigieg, S, Novillo-Ortiz, D, Sutherland, E, Anderson, M, de Witte, B, Peolsson, M, Unim, B, Pavlova, M, Stern, AD, Mossialos, E & van Kessel, R (2024) 'Mapping the regulatory landscape for artificial intelligence in health within the European Union, npj Digital Medicine, 7(229), p. 2.
61. Office of the Australian Information Commissioner (2025) Australian Privacy Principles, Australian Government, Canberra. Available at: <https://www.oaic.gov.au/privacy/australian-privacy-principles> (Accessed: 17 August 2025).
62. Protective Security Policy Framework (2025), Protective Security Policy Framework (PSPF), Australian Government. Available at: <https://www.protectivesecurity.gov.au> (Accessed: 8 January 2026).
63. Hosting Certification Framework (2025), Hosting Certification Framework, Australian Government. Available at: <https://www.hostingcertification.gov.au> (Accessed: 8 January 2026).
64. National Intermodal Corporation (2025), *National Intermodal - Transforming Australia's future supply chains*, NIC. Available at: <https://www.nationalintermodal.com.au> (Accessed: 23 August 2025).
65. NL Times (2024) 'Netherlands and Brazil to cooperate more closely against drug smuggling', 4 March. Available at: <https://nltimes.nl/2024/03/04/netherlands-brazil-cooperate-closely-against-drug-smuggling> (Accessed: 22 August 2025).
66. Australian Criminal Intelligence Commission (2025), *Report 24: National Wastewater Drug Monitoring Program*, ACIC, Canberra. Available at: <https://www.acic.gov.au/publications/national-wastewater-drug-monitoring-program-reports/report-24-national-wastewater-drug-monitoring-program> (Accessed: 8 January 2026).
67. Commonwealth of Australia (1901) *Customs Act 1901 (C'th)*, as amended by the *Customs Legislation Amendment (Controlled Trials and Other Measures) Act 2023*.
68. European Union (2024), *Regulation (EU) 2024/1689 (Artificial Intelligence Act)*.
69. Security of Critical Infrastructure Act 2018 (C'th), as amended by Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024 (C'th), Sch 3, s.5 (definition of "protected information.").
70. Customs Act 1901 (C'th), pt XII, ss. 203-214 (customs administration and data sharing provisions).
71. Biosecurity Act 2015 (C'th), Chapter 1, Section 5 (Appropriate Level of Protection; risk-based regulatory framework).
72. Australian Border Force Act 2015 (C'th), pt. 2, ss. 4-6, (functions and powers of the Australian Border Force and statutory authority for cross-agency enforcement and coordination).
73. Anti-Money Laundering and CounterTerrorism Financing Act 2006 (C'th), pt.2, ss.35-54 (identification, reporting and compliance programs).
74. Public Service Act 2020, New Zealand, Schedule 2, Part 3 – Border Executive Board (inserted by Public Service (Border Executive Board) Order 2020).
75. Department of Infrastructure, Transport, Regional Development, Communications and the Arts 2025, Guidance for new and redeveloping international port operators, Australian Government. Available at: <https://www.infrastructure.gov.au/infrastructure-transport-vehicles/maritime/international-port-operators> (Accessed 23 August 2025).
76. Sydney Airport Corporation 2025, 'New SmartGate kiosks go live at Sydney Airport fast-tracking international arrivals', Sydney Airport. Available at: <https://www.sydneyairport.com.au/corporate/media/corporate-newsroom/new-smartgate-kiosks-go-live-at-sydney-airport-fast-tracking-international> (Accessed 23 Aug.2025).
77. *Future Made in Australia Act 2024 (C'th)*. Available at: https://www.austlii.edu.au/cgi-bin/viewdb/au/legis/cth/num_act/fmiaa2024119 (Accessed: 10 January 2026).
78. Australian Government (n.d.) *Modern Manufacturing Initiative – Manufacturing Integration*. Available at: <https://business.gov.au/grants-and-programs/modern-manufacturing-initiative-manufacturing-integration> (Accessed: 10 January 2026).
79. Australian Government Department of Health and Aged Care (n.d.) *Medical Research Future Fund (MRFF): About*. Available at: <https://www.health.gov.au/our-work/mrff/about?language=en> (Accessed: 10 January 2026).



Australian
National
University

NATIONAL
SECURITY
COLLEGE

Contact

national.security.college@anu.edu.au

nsc.anu.edu.au

🐦 @NSC_ANU

🌐 ANU National Security College

📺 @anunationalsecuritycollege

✉️ @nscanu.bsky.social

CRICOS Provider #00120C

TEQSA Provider ID: PRV12002

(Australian University)



Subscribe to our mailing list

Scan the QR code or visit tinyurl.com/nsc-newsletters



Subscribe to the National Security Podcast

Scan the QR code or visit tinyurl.com/NatSecPod-NSC