29 AUGUST 2025

Charting New Horizons: Developing Horizon 2 of Australia's Cyber Security Strategy

Submission to the Department of Home Affairs on behalf of Freight &Trade Alliance (FTA) and the Australian Peak Shippers Association (APSA)

"KEEPING AUSTRALIA'S INTERNATIONAL TRADE MOVING"

FTA FREIGHT & TRADE ALLIANCE

Australian Peak Shippers Association Inc. (APSA)

Table of contents

ABOUT THE ALLIANCE

Freight & Trade Alliance (FTA) is the peak body for the international trade sector with a vision to establish a global benchmark of efficiency in Australian biosecurity, border related security, compliance, and logistics activities.

FTA represents more than 500 businesses including Australia's leading customs brokerages, freight forwarders and major importers.

On 1 January 2017, FTA was appointed the Secretariat role for the Australian Peak Shippers Association (APSA).

APSA is the peak body for Australia's containerised exporters and importers under *Part X of the Competition and Consumer Act 2010* as designated by the Federal Minister of Infrastructure and Transport.

APSA is also a member and has board representation on the Global Shippers Forum (GSF) that represents shippers' interests and that of their national and regional organisations in Asia, Europe, North and South America, Africa and Australasia.

FTA / APSA also provide international trade and logistics advocacy support to the following associations:

- Australian Council for Wool Exporters and Processors;
- Australian Dairy Products Federation;
- Australian Horticulture Trade;
- Australian International Movers Association;
- Australian Meat Industry Council;
- Australian Steel Association; and
- Tyre Stewardship Association.

The current APSA Officers and Committee of Management are listed below:

- Olga Harriton (Manildra Group) - APSA Chair
- Brian Thorpe (Visy) - APSA Vice Chair
- Billy Davies (Australian Meat Industry Council) - Treasurer
- Mark Christmas (QMAG)
- Flaminio Dondina (Casella Family Brands)
- Sarah Granger (Fletcher International Exports)
- Brian Wright (Australian International Movers Association)
- Michael Brittain (AGT Foods Australia)
- Paul Zalai - APSA Secretary

A list of all members and further information about FTA / APSA is available at www.FTAlliance.com.au

EXECUTIVE SUMMARY

Freight & Trade Alliance (FTA) and the Australian Peak Shippers Association (APSA) represent leading exporters, importers, and logistics providers, supported by skilled freight forwarders and licensed customs brokers who ensure Australia's supply chains function securely and efficiently. Our members manage sensitive trade and regulatory data on a daily basis, making them both critical to the national economy and uniquely exposed to cyber risks.

Cyber security for this community is not an abstract technology issue but a matter of supply chain continuity. A single disruption — whether caused by ransomware, compromised vendor platforms, or failures within government systems — can immediately halt cargo flows and undermine border clearance. This has downstream impacts on manufacturers, retailers, and consumers across the country.

The year 2025 also marks the twentieth anniversary of the Integrated Cargo System (ICS). While ICS has remained stable, its reliance on "ancient code" is well documented.

Its vulnerability to cyber-attack or unscheduled failure poses one of the greatest risks to trade continuity. Modernisation of ICS — or its staged replacement with a secure, resilient successor — must be a Horizon 2 priority.

Forwarders and customs brokers are also dominated by small and medium-sized enterprises, many of which lack the capacity to absorb the costs of cyber uplift. Programs such as Cyber Wardens provide a useful model, but sector-specific initiatives — for example, a "Cargo Cyber Wardens" scheme — are needed to equip frontline staff handling ICS entries, biosecurity declarations, and port system access. Affordable cyber insurance and practical ransomware playbooks would further strengthen resilience.

This submission also highlights the need for a freight/logistics Information Sharing and Analysis Centre (ISAC) to close a critical gap in threat intelligence, stronger standards for vendor platforms and cargo IoT devices, and harmonisation of overlapping compliance frameworks that currently drain SME resources.

In conclusion, FTA/APSA recommend that Horizon 2 place the freight forwarding and customs brokerage community at the centre of Australia's cyber resilience planning. Our sector handles the digital keys to Australia's trade. Protecting these businesses is essential to safeguarding both border security and the continuity of national supply chains.

CONTACT

For further detail please contact:

[redacted]

RECOMMENDATIONS

RECOMMENDATION 1 – Urgently invest in the cyber hardening or replacement of ICS

RECOMMENDATION 2 – Establish a freight/logistics ISAC for real-time sector-specific cyber threat sharing.

RECOMMENDATION 3 – Tailor cyber awareness programs and resources to freight SMEs.

RECOMMENDATION 4 – Develop affordable cyber insurance suited to small forwarding/brokerage firms.

RECOMMENDATION 5 – Mandate secure standards for cargo community systems and IoT devices used in freight.

RECOMMENDATION 6 – Harmonise overlapping compliance obligations across border and freight regulators.

RECOMMENDATION 7 – Embed cyber training into Chain of Responsibility frameworks.

RECOMMENDATION 8 – Support secure digital trade standards (MLETR, WCO, APEC) to strengthen international resilience.

RESPONSES

Q1. What trends or technology developments will shape the outlook under Horizon 2?
The sector is undergoing rapid digitisation. Electronic bills of lading, phytosanitary certificates, and customs declarations are increasingly mandatory, creating new efficiencies but also multiplying cyber attack surfaces. Artificial intelligence is being integrated into clearance and routing decisions, which may streamline operations but introduces risks if models are manipulated.

Australian forwarders and customs brokers are also tied into overseas platforms such as the EU's ICS2 and the US ACAS. A failure or breach in those systems would directly impact Australian trade, highlighting the global interdependence of cyber resilience. The Integrated Cargo System (ICS), turning 20 this year, is the most critical risk. It is indispensable to border clearance but reliant on outdated code. If compromised, trade would grind to a halt.

Q3. Does the high-level model resonate and do you have suggestions for refinement?
The model provides a strong foundation but does not yet capture the operational reality of freight. For forwarders and customs brokers, resilience is defined by whether they can still lodge cargo reports in ICS, process declarations, and ensure cargo movement during a disruption.

Q4. Can you suggest ways to collect data and feedback to monitor these outcomes?
ICS system logs and port community data already provide visibility into throughput and failures. These can serve as resilience indicators. The Single Reporting Portal is also valuable, but it requires greater promotion within the freight sector.

Q5. What could government do to better target and consolidate its cyber awareness message?
Awareness messaging must be delivered through compliance channels already used by freight forwarders and customs brokers. ABF notices, DAFF circulars, and FTA/APSA updates are trusted sources. General campaigns often fail to cut through.

Sector-specific case studies are essential:

- Phishing emails that impersonate shipping lines or regulators.
- Ransomware attacks that lock forwarding software.
- Fraudulent invoices leading to cargo delays.

Embedding these examples into compliance updates ensures the message reaches the right audience.

Q7. How can Government encourage SMBs to uptake existing cyber resources?
Most forwarders and customs brokers are SMEs. They face constant compliance obligations and thin margins, which limit investment in cyber resources. Uptake will improve if:

- Training and self-assessments are tied directly to cargo reporting processes.
- Incentives such as reduced compliance fees or recognition programs are offered.

Embedding cyber into existing workflows avoids duplication and ensures engagement**.**

Q8. How can industry and government work together to drive uptake of cyber actions by SMEs?
Partnership is key. Freight-specific resources must be co-designed by government and industry. This could include:

- Cyber playbooks tailored to forwarding and customs operations.
- Subsidised access to secure documentation platforms for SMEs.
- Pilot programs that demonstrate cost-effective resilience measures**.**

Q9. What standards could assist cyber uplift for SMBs?
The Essential Eight is a good baseline but needs sector-specific adaptation. Freight forwarders and customs brokers would benefit from a tailored standard that:

- Focuses on systems central to cargo reporting and clearance.
- Aligns with Chain of Responsibility frameworks, making compliance clear and enforceable.

Q11. Is cyber insurance affordable and accessible for small entities?
No. Cyber insurance is generally priced out of reach for small forwarders and customs brokers. Premiums are high and requirements complex, leading many to forgo coverage.

Q12. How well do you understand ransomware?
FTA/APSA members have experienced ransomware first-hand, particularly targeting forwarding platforms. Attacks increasingly mimic ABF or shipping line communications. For SMEs, the consequences are severe:

- Cargo clearance is delayed.
- Costs escalate rapidly.
- Customer trust is damaged.

Q13. How could government further support businesses against ransomware?
Develop a Logistics Ransomware Playbook providing:

- Step-by-step incident response guidance.
- Contact protocols for ABF, DAFF and other regulators.
- Practical strategies for maintaining cargo flow while systems are compromised.

Q14. Have you experienced vulnerabilities or impacts from incidents that disproportionately affect your sector?
Yes. Forwarders and customs brokers are heavily reliant on third-party vendor platforms, many of which are managed offshore. When these systems are disrupted, cargo lodgement and clearance stop immediately. ICS outages have also demonstrated how concentrated the risk is: a single point of failure can paralyse national trade.

Q16. Which regulations are most important in reducing cyber risk?
The SOCI Act has lifted standards for major infrastructure operators but leaves critical gaps for cargo community systems and offshore vendor platforms. These platforms handle sensitive cargo data yet remain outside the framework.

Q17. Have compliance requirements negatively impacted your cyber maturity?
Yes. Forwarders and customs brokers face overlapping regulatory obligations across ABF, DAFF, aviation, and maritime. For SMEs, this diverts resources away from cyber investment.

Q18. What international best practice should Australia consider for secure tech standards?
The EU's Cyber Resilience Act demonstrates how baseline security standards can be mandated for IoT devices. For freight, this should apply to:

- Container trackers.
- Reefer monitors.
- Smart seals and access cards.

Mandatory requirements for patching, secure defaults, and vulnerability disclosure would reduce systemic supply chain risk.

Q19. How should government help end-users be informed about cyber risks in products?
End-users in freight are operators selecting forwarding platforms and cargo systems. A certification or labelling scheme for secure freight IT products would provide clarity and allow informed decisions.

Q20. What guidance is needed on foreign vendor risks?
Some forwarding and cargo systems are owned offshore. Forwarders and customs brokers often lack visibility into their governance or security standards. Government guidance should provide:

- Clear due diligence checklists.
- Indicators of unacceptable risk.
- A framework of approved or trusted vendors.

Q21. How could government and industry better understand data flows?
Trade generates complex data flows — manifests, declarations, certificates — much of which is routed offshore. Mapping these flows with industry involvement would identify vulnerabilities and highlight where additional protections are needed.

Q22. How can secure data sharing enable innovation?
Industry is keen to adopt innovations such as electronic bills of lading and AI-driven clearance, but trust in data security is essential. A joint governance framework, co-developed with industry, would give forwarders and customs brokers confidence to innovate securely.

Q23. What guidance would support safe adoption of emerging technologies?
Forwarders and customs brokers need practical, freight-specific case studies demonstrating how to safely adopt:

- Electronic bills of lading.
- AI for customs compliance.
- IoT cargo monitoring.

Guidance must highlight compliance obligations, cyber risks, and mitigation strategies.

Q24. What could government do to support a more proactive cyber posture?
Government should fund joint cyber exercises with freight forwarders and customs brokers, publish sector-specific playbooks, and provide real-time alerts relevant to freight threats such as phishing campaigns and invoice fraud.

Q26. How could government further support industry to block threats at scale?
Establish a freight/logistics ISAC, enabling real-time sharing of cyber intelligence between forwarders, customs brokers, government, and trusted partners.

Q28. What more is needed to support a thriving threat-sharing ecosystem?
Freight has no structured cyber threat-sharing mechanism. A dedicated ISAC would close this gap and bring the sector into alignment with higher-maturity industries such as finance.

Q29. How can intelligence sharing for scams prevention be improved?
Sharing must focus on freight-specific threats, such as:

- Phishing emails posing as shipping lines.
- Fake ABF/DAFF notices.
- Malicious attachments disguised as cargo documents.

Q30. Are roles clear in a cyber conflict or crisis?
Not from the freight perspective. Forwarders and customs brokers require clarity on who leads response if ICS or other critical cargo systems are compromised. Crisis exercises should include the sector to establish clear protocols.

Q32. Does Australia need a vulnerability disclosure program?
Yes. Vulnerabilities in freight software are often discovered externally. A safe disclosure channel would allow fixes before they are exploited.

Q33. How effective is the SOCI Act?
It has improved standards for ports and terminals but leaves dependent SMEs — including forwarders and customs brokers — outside its scope. These businesses remain critical yet unsupported.

Q34. Are there risks not addressed under the current framework?
Yes. Cargo community systems and offshore vendor platforms remain outside regulatory coverage, despite being essential to the flow of trade.

Q35. Is the regulatory burden proportionate?
For large operators, yes. For SMEs such as forwarders and customs brokers, the indirect burden of aligning with multiple compliance regimes reduces capacity for cyber investment.

Q36. What support would assist operators to mature resilience?
Practical resources such as checklists and incident response templates would help SMEs. Targeted grants or credits could offset costs of cyber uplift for smaller forwarders and customs brokers.

Q38. How can Australia strengthen its sovereign cyber workforce?
Cyber awareness should be embedded in Chain of Responsibility training, ensuring it reaches all freight professionals. Subsidised apprenticeships and training programs for logistics-specific cyber roles would also address workforce gaps.

Q40. How do we better support SMEs to access sovereign cyber capabilities?
SMEs cannot sustain dedicated cyber teams. Shared-service hubs or government-supported platforms would give forwarders and customs brokers affordable access to expertise.

Q42. How can government and industry promote Australia's sovereign cyber capabilities internationally?
By leading in secure digital trade. Adoption of MLETR-compliant systems would demonstrate Australian leadership and open opportunities for exporting trusted trade technologies.

Q44. How should Australia position itself in international cyber norms and standards?
Australia should champion secure digital trade standards, ensuring electronic bills of lading and cargo systems are developed with cyber resilience at their core.

Q49. What role should Australia play in shaping global standards for emerging technologies?
Australia should lead in setting secure standards for freight technologies such as electronic bills of lading and cargo IoT devices. This positions us as a trusted trade partner.

Q50. Are there forums Australia should prioritise?
APEC, ASEAN, and the World Customs Organization are the most relevant forums for embedding cyber resilience in trade systems and ensuring harmonisation across borders.

Conclusion

Freight forwarders and customs brokers sit at the heart of Australia's international supply chains, ensuring compliance, facilitating border clearance, and managing the digital documentation that underpins trade. This makes them indispensable to economic security — and uniquely vulnerable to cyber risk.

The consultation questions we have addressed highlight a consistent theme: cyber resilience in freight is not a "nice to have" but a prerequisite for national continuity. For our members, the reality of cyber security is measured not in abstract frameworks but in whether cargo can still be reported, cleared, and delivered.

The twentieth anniversary of the Integrated Cargo System (ICS) is a timely reminder that Australia cannot rely indefinitely on ageing infrastructure. Horizon 2 must secure ICS and the wider trade ecosystem while providing practical, affordable support for the small and medium-sized enterprises that dominate our sector.

FTA and APSA stand ready to work in partnership with government to deliver these outcomes. By prioritising the resilience of freight forwarders and customs brokers, Horizon 2 can safeguard Australia's trade flows, strengthen border security, and ensure our supply chains remain competitive and trusted in an increasingly uncertain global environment.