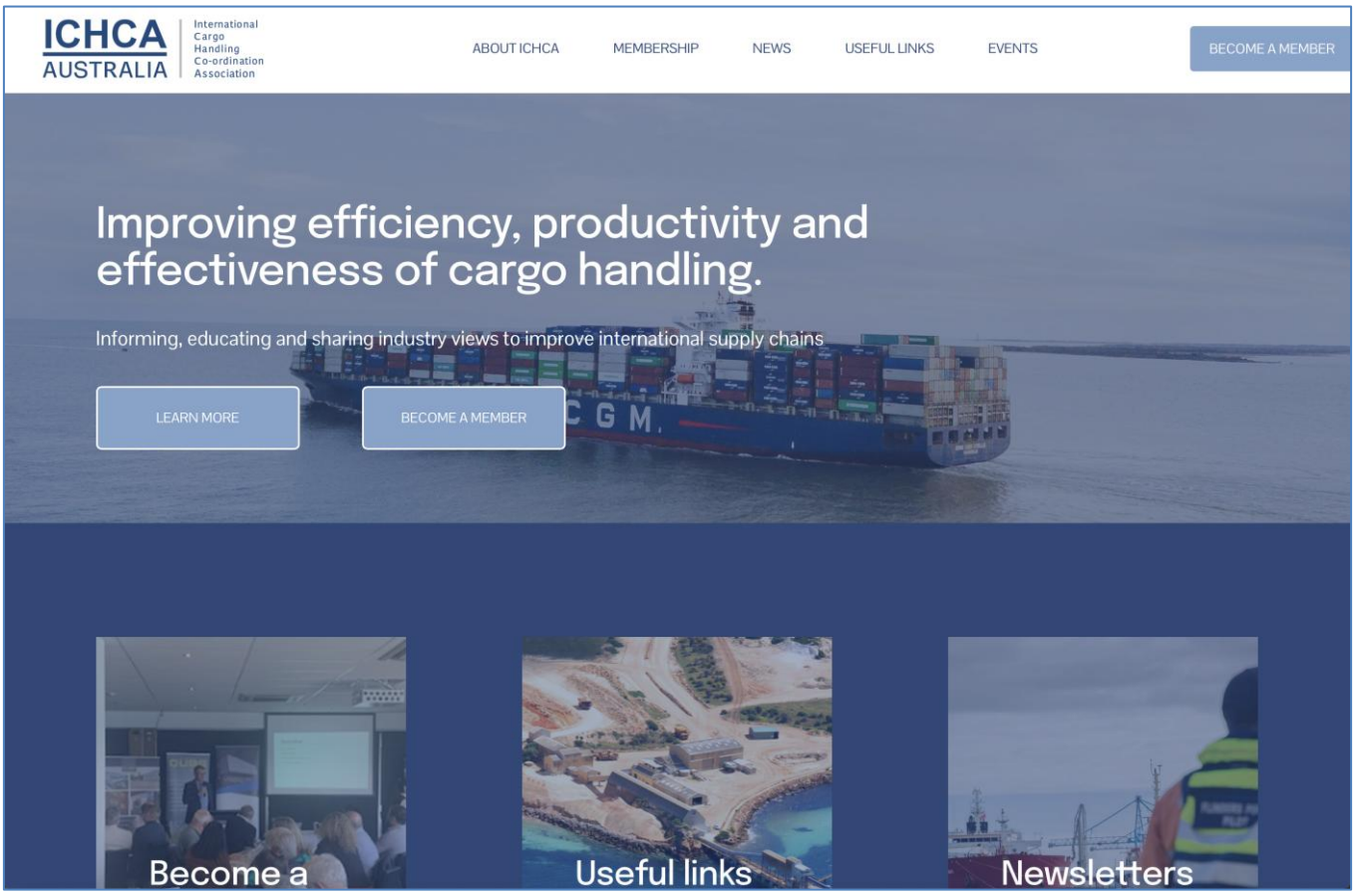
About ICHCA – International Cargo Handling Co-ordination Association

The International Cargo Handling Co-ordination Association (ICHCA) is an international, independent, not-for-profit organisation dedicated to improving the safety, security, sustainability, productivity and efficiency of cargo handling and goods movement by all modes and through all phases of national and international supply chains. ICHCA International's privileged non-government organisation (NGO) status enables it to represent its members, and the cargo handling industry at large best, in front of national and international agencies and regulatory bodies. Its Expert Panel provides practice advice and publications on a wide range of practical cargo handling issues. ICHCA Australia Ltd is proud to be part of the ICHCA International Ltd global network (**www.ichca.com**). To access past newsletters and other useful information go to the ICHCA Australia website at **www.ichca.com.au.**

Inside this issue

ICHCA Australia launches new website

ICHCA Australia's new website can be found at: **www.ichca.com.au.** Have a look and send us your comments. Any ideas for improvements are also welcome.



Port of Melbourne draft port development plan out for comment

The Port of Melbourne (PoM) recently released its **Draft 2055 Port Development Strategy (Draft 2055 PDS)** for stakeholder comment. According to the report's introduction, the Draft 2055 PDS outlines the high-level plans and approach for developing the capacity and efficiency of the Port for the next 30 years, while also providing a planning framework that is adaptable and responsive to changing needs over time.

Under the Port Management Act 1995 (Vic), all Victorian ports are legislatively required to have a PDS and to review it every five years. Following its review of the 2050 PDS published in 2020, PoM is now developing the 2055 PDS, due to be completed by December 2025.

The Draft 2055 PDS has been shaped by stakeholder engagement that included surveys to understand stakeholders' engagement preferences, 1:1 meetings with key tenants and port users, workshops with industry, community and government, and a written request for stakeholders' input. PoM is now inviting formal submissions from stakeholders between 14 April and 6 June 2025 to provide feedback on the Draft 2055 PDS.

To help facilitate stakeholders' submissions, PoM is hosting a series of stakeholder briefings and 1:1 meetings, to meet its commitment to keeping stakeholders up to date. Formal responses will be provided to all submissions.

See here for further details.

Massive explosion at Bandar Abbas

At least 65 people have been killed and over 1,200 injured in a massive explosion at one of Iran's key ports, authorities said last Monday. Firefighters are still battling the blaze that Iranian officials say was under control 48 hours after the start of the fire.

Source: AP

The blast took place in the Shahid Rajaee section of the port near the southern city of Bandar Abbas, Iran's biggest container hub.

Efforts to put out the ensuing blaze have continued, since sporadic fires have broken out due to wind and flammable goods in the containers, some releasing toxic emissions. The blast blew out windows and roofs of nearby buildings and destroyed cars. Residents reported feeling the impact of the blast up to 50 km away.

One private maritime risk consultancy said it believed the affected containers had contained solid fuel destined for ballistic missiles. The fire was the result of "improper handling of a shipment of solid fuel intended for use in Iranian ballistic missiles", Ambrey Intelligence said. Ambrey added that it was aware that an Iran-flagged ship "discharged a shipment of sodium perchlorate rocket fuel at the port in March 2025".

State media quoted witnesses as saying the explosion occurred after a fire broke out and spread to unsealed containers storing "flammable materials". Customs officials later released a statement, reported by Iranian state TV, saying the explosion had probably resulted from a fire that had broken out in a hazmat and chemical materials storage depot. In a later update, Ambrey quoted Iran's National Disaster Management Organisation as saying officials had previously issued warnings to Shahid Rajaee port regarding the safe storage of chemicals.

Shahid Rajaee port is Iran's largest and most advanced terminal, through which much of the country's sea-borne cargo transits.It is located on the Strait of Hormuz, a major shipping channel for oil cargo, and is about 20 km west of Bandar Abbas, Iran's major port city on its south coast and home to the Iranian Navy's main base. Iran's national oil production company said the explosion at the port had "no connection" to the country's oil refineries, fuel tanks or pipelines, local media reported.

The Port of Darwin ownership tussle

The Port of Darwin is likely to return to Australian ownership no matter who wins the federal election, after both the Coalition and Labor pledged to negotiate a deal. The port has been in a Chinese company's hands after the Northern Territory government awarded a 99-year lease to Beijing-controlled Landbridge Group in 2015, under a deal approved by the then-Turnbull government.

Citing the current geo-political environment, the Coalition said it would force Landbridge Group to sell back the port to an Australian government-approved operator, or as a last resort compulsorily acquire it and compensate the Chinese-owned company. Mr Albanese also flagged recently that his government was considering options to end the port's lease. He declined to detail how much his government would be willing to pay. Landbridge non-executive director Terry O'Connor stated that they have not had any discussions with the federal government or the NT government "As far as the owner is concerned, there's no intention to sell the port and there's been no negotiations around selling the port," he said.

Cyber security considerations for Australian agriculture supply chains

In recent years, Australian agriculture has seen considerable growth in investment in technology (often referred to as "Agtech"). Agtech, including artificial intelligence (AI) tools, digital agronomy and precision agriculture hardware, together with the digitisation of contract management and trade, have advanced the industry. Benefits of Agtech include increased productivity, enhanced sustainability, reductions in costs and improvements in efficiency. The market for AI tools in the global agriculture industry is set to grow from US$1.7 billion in 2023 to US$4.7 billion by 2028, highlighting the increasing role of technologies in the sector and signalling a period of transformation.

Increased digitisation also creates greater opportunity for criminals to target individual businesses – and supply chain vulnerabilities – through cyber attacks. Over the past five years, the Australian agriculture industry has faced major cyber attacks affecting the grain, beef and wool trades, resulting in considerable disruption and substantial financial losses. As such, it is clear that the technological advancements across the agriculture sector demand a corresponding increase in cybersecurity for all stakeholders across supply chains.

Cyber security risk management has therefore become central to business operations and, where needed, expert advice from specialised cybersecurity companies and consultants should be considered to ensure optimal risk mitigation. An effective cyber security plan – including a cyber incident response strategy – is critical to minimising disruption and potential financial losses.

Cyber security risk manafgment plans

Risk management plans are likely to include a number of straightforward practical actions, including:

- Installing firewalls and third party anti-virus software
- Enabling multi-factor authentication
- Downloading software updates promptly
- Restricting access to sensitive data and documents
- Utilising cloud storage
- Using a password manager
- Utilising external hard drives to back up data
- Using secure payment platforms

From a legal and compliance perspective, we recommend that clients consider the following:

Staff Training: Human beings can be the vulnerable link in an organisation because a subtle change is hard to spot, particularly in familiar and routine messages which are perhaps not scrutinised in detail. Training to identify phishing attacks and establishing good practices such as checking with a counterparty on receipt of new account details can prevent attacks from succeeding.

Third Party Providers: Another vulnerability can be third party providers. If you use brokers or agents, it would be advisable to conduct due diligence on their cyber security protection and, where possible, require them to obtain a recognised cyber security certification. Many trading companies and banks now place a greater emphasis on information and cyber security in their onboarding processes.

Contractual counterparties: As well as protecting your own organisation, in some circumstances where regular or high value trading is involved, and depending on your commercial bargaining power, you may also want to consider including an express contractual requirement that your counterparties obtain recognised cyber security certification.

Contractual protections: The allocation of risk if a phishing attack succeeds can be expressly agreed in your contracts in advance. A number of traders are introducing clauses into their standard form contracts that specifically require counterparties who receive a request to make payment to a new account to independently verify the new account details with their usual contact. Whilst this ought to form part of

standard good practice in any event, such clauses seek to allocate risk if a party makes payment to an unverified account without conducting the contractually mandated checks.

Recent case law

The importance of what parties agree in their contracts is illustrated by a 2019 England & Wales court judgment, *K v A* [2019] EWHC 118 (Comm).

A contracted to sell sunflower meal to *K* on a FOB basis under GAFTA Form 119. *A* used a third party intermediary broker, *V*. After loading the goods, *A* sent *V* two emails with invoices and bank account details for payment and *V* forwarded them to *K*. *K* denied receiving these emails – instead, it received emails appearing to come from *V* with attachments directing payment to the right bank but to a different account. Without realising that a fraud was underway (and without checking), *K* made payment to the different account. Once the fraud was discovered, payment was made to the correct account but with a shortfall caused by currency conversions. *A* claimed the shortfall against *K* in a GAFTA arbitration which was ultimately appealed to the English Commercial Court.

At first instance, the tribunal had ruled that the loss should be borne by the party whose account was hacked (being *A*). On appeal, the GAFTA Board of Appeal held that under clause 18 of GAFTA 119, the emails with the correct account details sent by *A* to *V* constituted good notice. *K* therefore bore the risk of receiving the wrong account details. *A* had sent valid and correct notices and *K* had failed to pay.

K appealed to the English Commercial Court. Ultimately, the Court focused on the contractual payment obligation, which was to pay the price in "net cash: to *A*'s bank within 2 days of presentation of documents, which must include a commercial invoice". It held that the contractual obligation was to make payment to *A*'s bank for *A*'s account in the sense that it must be accompanied by the account details which *A* had notified. *K* had failed to do this and so *K* carried the risk of the loss.

HFW Comment

The best protection is to take steps in advance – both practical and legal – to prevent cyber attacks and/or to minimise the risk of damage. Preparedness is key.

This article was supplied by HFW, sponsor of Inside ICHCA.

US withdraws from IMO marine environment discussions

At the recent International Maritime Organization's (IMO's) Marine Environment Protection Committee (MEPC) meeting in London, the Trump administration announced the US withdrawal from crucial maritime decarbonisation negotiations.The US government delivered a strongly worded message to IMO delegations, explicitly rejecting any measures that would impose fees on US vessels based on greenhouse gas emissions or fuel choice. The administration further warned it would consider implementing reciprocal measures to offset any charges imposed on American ships.

The IMO's Net-Zero Framework plans to modify MARPOL Annex VI by implementing both a marine fuel standard and emissions pricing system. The 2023 IMO GHG Strategy aims to achieve net-zero emissions from international shipping by 2050, with emissions peaking as soon as possible, while considering national circumstances and aligning with Paris Agreement temperature goals.

In its message, the Trump administration characterised the IMO's efforts as "an attempt to redistribute wealth under the guise of environmental protection". The US particularly objected to the IMO's goal of achieving net-zero emissions by 2050, arguing it would "unwisely promote the use of hypothetical expensive and unproven fuels".

The IMO's current strategy further aims for a 40% reduction in shipping's carbon intensity by 2030 compared to 2008 levels, with 5-10% of shipping's energy coming from zero or near-zero GHG emission

sources by 2030. If approved, these measures could become effective in 2027 following final adoption at an extraordinary MEPC session in October 2025.

Patricks Teminals rolls over Enterprise Agreement

Patrick Terminals has secured a roll-over agreement with the Maritime Union of Australia (MUA) and its employees to extend the company's Enterprise Agreement until the end of 2028. The Enterprise Agreement will now be submitted to the Fair Work Commission for approval.

Patrick Terminals CEO Michael Jovicic has welcomed the agreement, saying:

> This historic agreement roll-over provides a strong foundation for the future, ensuring stability for our employees and certainty for our customers in an increasingly dynamic global environment. As a trusted Australian container terminal operator, we remain committed to delivering resilient and reliable services to our quayside and landside customers.

Patrick Terminals says the agreement underscores the company's "ongoing commitment to productive workplace relations". The roll-over agreement will run until 31 December 2028 if approved.

Ningbo Port incident report released

The China Maritime Safety Administration (CMSA) recently published a report on its investigation into the explosion and subsequent fire on the Taiwanese-owned container vessel *YM Mobility* at China's Ningbo Port on 9 August, 2024. On that date, an explosion occurred in a container loaded with dangerous goods near the ship's bow. According to the shipper's declaration, the container was a reefer used as a substitute for a dry container, without requiring power connection. The estimated economic loss resulting from in the incident was about CNY90 million (US$13 million).

The CMSA determined that the cargo in the affected reefer container included tert-Butyl peroxybenzoate (TBPB), a compound that has thermal instability and can self-decompose at room temperature, thus releasing a large amount of heat and producing gas or vapour. The unplugged reefer was used to store TBPB despite having poor heat dissipation properties. The heat generated by the TBPB self-decomposition reaction therefore accumulated in the reefer.

The continuous increase in temperature accelerated the self-decomposition reaction, which then resulted in thermal runaway and the subsequent explosion and fire. The CMSA also determined that the incident occurred during a period when summer temperatures in Shanghai, where the TBPB was packed, were

higher than usual. On July 25, during the packing of the TBPB cargo, the packing temperature was consistent with the ambient temperature (about 35° Celsius). From 25 July to 9 August, Shanghai and Ningbo continued to experience high temperatures, with the highest daytime temperature reaching about 40° Celsius, and the outside temperature of the containers stacked in the open air was even higher.

The investigation showed that the operator failed to exercise sufficient care when reviewing the cargo transportation plan. In particular, the operator failed to conduct a full safety assessment of the stability of the cargo and the risk of thermal runaway in view of the actual conditions, such as high summer temperatures, self-separation of the cargo, and thermal insulation of the unplugged reefer. The operator had agreed to use the unplugged reefer to transport the dangerous goods and so did not consider the temperature changes in the container during transportation.

The CMSA said it had found no abnormalities in other steps throughout the cargo transportation process. The investigation team determined that the shipper and the operator had chosen to use an unplugged reefer to transport TBPB. When the two parties agreed, selected and reviewed the TBPB transportation plan, they failed to take sufficient caution to combine the risk factors such as the high temperatures at that time, the heat release characteristics of the self-decomposition reaction of the cargo, and the thermal insulation and airtightness of the unplugged reefer. They also did not fully study and judge the possible safety risks in the process of packing and transportation.

The investigation team found that both the operator and the shipper were responsible for the incident.

Port Botany DP World terminal berth extension

NSW Ports has proposed a berth extension at the DP World Container Terminal.

The project will provide equivalent quayline length for each container stevedore company operating at Port Botany.

The investment in additional quayline will ensure Port Botany, which is NSW's container port, can continue to efficiently meet the trade needs of NSW. All three container terminals will then have the capability to berth three longer container vessels at the same time, improving port operations.

An artist's impression of the project once completed. Source: NSW Ports

The project includes extending the southern quay of Brotherson Dock by 314 metres, with adjoining hardstand area to enable ships to be loaded and unloaded. In order to extend the quayline, NSW Ports will be relocating Bulk Liquids Berth 1 to the south of Bulk Liquids Berth 2.

NSW Ports has stated that it will engage with the community throughout the planning process, including through the long-standing Port Botany Community Consultation Committee as well as broader public consultation.

Updates from the Department of Agriculture, Fisheries and Forestry

DCCC meeting

The Department of Agriculture, Fisheries and Forestry Cargo Consultative Committee (DCCC) brings together DAFF and industry representatives to address biosecurity issues impacting trade and logistics with the purpose of ensuring effective biosecurity regulation without unnecessary trade barriers.

The last meeting of the DCCC was held on 3 April 2025. Please notify Peter van Duyn if you would like a copy of the minutes of the meeting. ICHCA Australia is also represented on the the Imported Sea Container Pathway Working Group which deals with conatainer cleanliness and biosecurity issues.

BPL season ends

The 2024-2025 flight season of the Burnt Pine Longicorn (BPL) beetle concluded at 23:59 hours (NZST) on Wednesday 30 April 2025. Annual heightened surveillance regime for managing the risks posed BPL beetles on vessels departing New Zealand ceased from midnight, 24:00 hours (NZST) on 30 April 2025. Timber and timber products imported from New Zealand will no longer be subject to specific import requirements that are applied during the BPL flight season.

New Methyl Bromide Fumigation Methodology now in force

Version 3.0 of the Methyl Bromide Fumigation Methodology is now in effect. You can find the new version on the department's methodologies and documents for biosecurity treatments webpage to ensure you are meeting the new requirements and conducting fumigations correctly.

All methyl bromide fumigations with a start date and time at or after 1 May 2025 00:00 (midnight local time) must adhere to the new requirements. Local time means the place where the fumigation was performed.

ICHCA Contacts

ICHCA Australia Chairman
Scott McKay
Mobile: 0411 042 130
Email: scott@flywheeladvisory.com.au

Company Secretary
Peter van Duyn
492 George St, Fitzroy VIC 3065
Mobile: 0419 370 332
Email: peter.van-duyn@ichca.com

State co-ordinators

New South Wales
Marcus John
Mobile: 0413 486421
Email: marcus.John@thomasmiller.com

South Australia
Michael Simms
Mobile: 0418 802 634
Email: Michael.Simms@fphgroup.com.au

Victoria
Peter van Duyn
Mobile: 0419 370 332
Email: peter.van-duyn@ichca.com

Queensland
Tim Polson
Mobile: 0427 426 910
Email: Tim.Polson@ligentia.global

ICHCA AUSTRALIA LIMITED (IAL) PRIVACY POLICY

IAL's Privacy Policy details are available by contacting the Company Secretary, Peter van Duyn, via e-mail peter.van-duyn@ichca.com or telephone 0419 370 332.

Our contact with you

If you do not wish to receive further copies of this newsletter, please advise peter.van-duyn@ichca.com and the distribution will be cancelled. If you wish to have it sent to other people in your organisation or contacts in the cargo handling industry, please advise us.