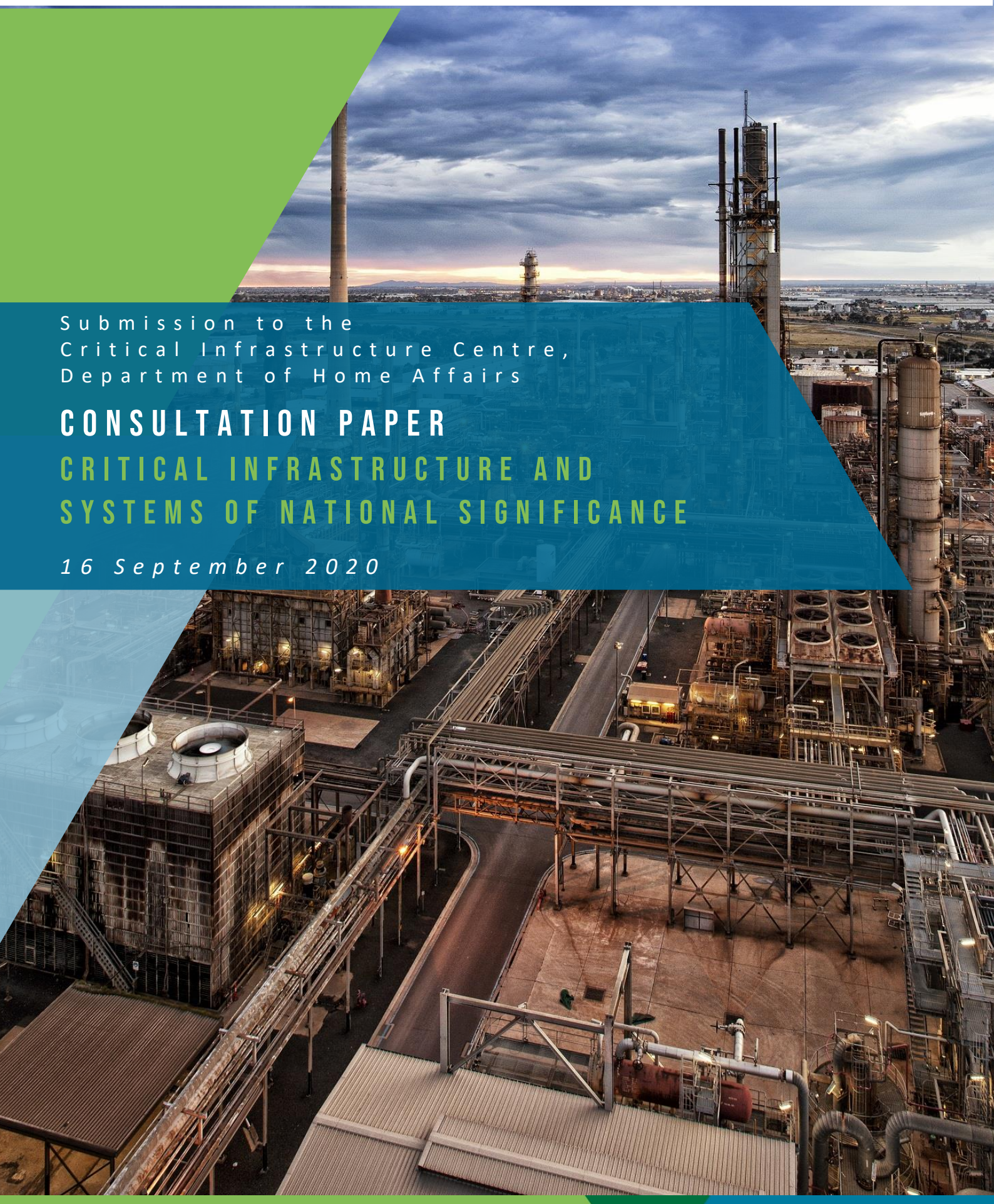
Australian Institute of Petroleum



Submission to the
Critical Infrastructure Centre,
Department of Home Affairs

CONSULTATION PAPER

CRITICAL INFRASTRUCTURE AND SYSTEMS OF NATIONAL SIGNIFICANCE

16 September 2020

CONTENTS

AUSTRALIAN INSTITUTE OF PETROLEUM LTD
42 Macquarie Street, Barton ACT 2600 | GPO Box 279, Canberra ACT 2601
ABN 11 005 152 581 **T** +61 2 6247 3044 **E** aip@aip.com.au **W** www.aip.com.au

EXECUTIVE SUMMARY: KEY MESSAGES & POSITIONS

- AIP member companies acknowledge the critical importance of reliable fuel supply - to their customers, communities, businesses, key Australian industries and Defence and emergency services.

- These companies have an enviable record of delivering this outcome - with no widespread or prolonged shortages experienced in decades, even during major global conflicts and supply disruptions from various sources.

- This vital industry imperative is directly aligned with the Government's objective of reliable fuel supply, which is delivered through a competitive market and a flexible and diverse network of infrastructure, transport options, fuel suppliers and personnel – contrasting with other energy sectors (see Section E).

- Direct alignment of objectives also exists to protect critical industry infrastructure, operational reliability, sensitive data and people from a range of operational, physical and cyber security threats. AIP members achieve this through meeting robust standards for risk identification, mitigation and response planning on commercial terms, supported by national and State emergency plans to manage widespread disruptions from different sources and affecting multiple market operators (Sections D&E).

- AIP member companies do acknowledge, however, that cyber security threats are persistent, evolving and increasingly severe, creating significant global challenges for governments and business to protect sensitive information, critical assets, the environment and the safety of the community.

- In this context, AIP member companies do support the Australian Government taking action to protect private companies from cyber attacks and providing strong deterrents against cyber-crime and nation state attacks. The issue then is the framework, scope and design of these Government actions.

- The proposed 'Enhanced Regulatory Framework' for Critical Infrastructure aims to "uplift resilience" of all critical infrastructure sectors through collaborative approaches and new government powers and a range of regulatory obligations, including applying these to a broader range of local industries.

- The industry supports the government in taking the lead in improving Australia's situational awareness, as this will strengthen the cyber security posture and capabilities of each organization operating in Australia. The key to achieving this is proactively identifying and remediating cyber vulnerabilities via information and intelligence sharing between public and private sectors.

- The fuels industry actively participates in and values open and collaborative emergency management and information sharing on vulnerabilities between government entities and private partners, within legal parameters including competition law and data privacy legislation, to help prevent and manage threats. The industry therefore welcomes many Consultation Paper initiatives (on page 15). However, AIP member companies support sharing of information on a voluntary basis, as opposed to mandatory disclosure, and full compliance with non-disclosure requirements unless agreed by entities.

- Beyond information sharing, new regulatory imposts (rather than incentive based self-regulation and audits favoured by industry) remain a major concern to the industry operating in a competitive market and needing to deliver competitive consumer fuel prices. This is particularly the case where the government's regulatory role does not align with the industry's cyber and data privacy programs.

- Concerns about regulatory imposts are magnified in the current environment – given ongoing financial impacts of COVID-19, the negative outlook for the local and global industry, and the Government's clear recognition of these impacts in recent welcome announcements and ongoing consultations with industry to address the ongoing viability challenges faced by Australian refineries (Section F).

- AIP member companies welcome the clear Government commitments in the Consultation Paper (Section C) to co-design and adopt proportional approaches to the preparedness and risks of specific sectors and entities, not impose unnecessary regulatory burdens, and deliver a real uplift in security *"whilst ensuring businesses remain viable and services remain sustainable, accessible and affordable".*

- However, there is much detail still to be developed and finalised, particularly for industry to be comforted that these Framework principles and objectives will be delivered in practice without unintended impacts and business costs.

- The entities and critical infrastructure to be covered by the Framework is a critical consideration. The cyber security laws and regulations applying globally are based on unique definitions and differences on what are considered 'Critical Infrastructure' (CI) in their respective countries (and based on each country's different national security and economic concerns and challenges).

- Therefore, to ensure that an infrastructure is truly critical in Australia, AIP member companies support clear terminology and criteria/thresholds being developed for the appropriate identification of CIs in the proposed Framework. In addition, where specific cybersecurity requirements apply to critical infrastructure, we support the use of clear terminology to ensure that only fuels related infrastructure that is truly critical, is treated as such.

- In relation to *Positive Security Obligations*, AIP member companies support in-principle incentive-based self regulation and audits (encouraged through legislation) to demonstrate the adequacy of companies' security measures. In this regard, we also support and would participate in the development of risk-based industry guidelines and existing public-private frameworks to protect against cyber threats.

- AIP members do not support, however, unnecessary mandatory or sanction-based security measures, which degrade (or disincentivise) ongoing cybersecurity investments by the industry and operators. This would occur where mandatory security measures or specific standards are imposed on individual AIP member companies despite being able to demonstrate that they have robust security measures and practices already established and there is a reasonable expectation of meeting security obligations.

- The choice of regulator for each sector will also be critical. While the proposed regulatory model would avoid duplication with existing oversight requirements and specific industry regulators would normally be in the best position to provide guidance to entities on how to meet their obligation, the suggested compliance and enforcement process by the regulators seems to be overly administrative and once again raises concerns of degrading ongoing industry investments in cybersecurity.

- In relation to 'Cyber Assistance for Entities', AIP member companies fully understand that in times of national emergency there may be a need for government to intervene and issue directions to support response and recovery actions. However, in most cases, AIP member companies believe in taking their own proactive action in responding to major cyber incidents and threats, and should be empowered to do so within the current and future legislative parameters and framework. Naturally the industry would seek Government assistance and be fully cooperative when necessary, but immediate direct intervention by the Government should be the last resort.

- Currently, the fuels industry is not regulated in this regard, with the Government instead relying on commercial approaches and protections and collaborative arrangements with industry. Therefore, the Enhanced Framework could represent material obligations and costs on the fuels industry depending on its final design and application. If the Government has national security objectives beyond commercial imperatives (to protect infrastructure, operations, working capital, staff and data), then government support should be provided to meet any additional costs of these government imperatives.

A. INTRODUCTION

The Australian Institute of Petroleum (AIP) welcomes the opportunity to provide a submission to this initial engagement and Consultation Paper. This consultation process is seeking views on the development and application of an 'Enhanced Regulatory Framework' to underpin the security and resilience of critical infrastructure and the ongoing supply of essential services across Australia.

This Submission is made by AIP on behalf of its core member companies – Ampol Limited, bp Australia Pty Ltd, Mobil Oil Australia Pty Ltd and Viva Energy Australia Pty Ltd.

These companies operate all four major oil refineries in Australia and supply around 90% of transport fuel to our local market via refinery production, imported supply and trading operations, and through their nation-wide fuel storage, terminal, distribution and retail networks.

Underpinning these supply chains is considerable industry investment in supply infrastructure, and a requirement for major ongoing investment in maintaining existing capacity. Over the last decade, AIP member companies have invested billions of dollars to maintain the reliability and efficiency of fuel supply meeting Australian quality standards.

AIP is the peak representative body representing these members and the downstream petroleum industry since 1976, and AIP's mission is to promote and assist in the development of a sustainable, internationally competitive petroleum products industry, operating safely, efficiently and economically, and in harmony with the environment and community standards.

As a non-profit making industry association, AIP is not an 'owner or operator of fuel supply infrastructure' and is therefore unable to respond to the very wide range of 'operator' and 'entity level' questions and legal considerations identified in the Consultation Paper. Individual AIP member companies may provide feedback and submissions themselves on these matters.

AIP can, however, provide information and advice to the Government on:

- overall market operation, conditions and impact analysis, including to avoid unintended consequences
- sound framework objectives and policy principles to meet government objectives
- coordination of industry technical support during the framework's development and implementation.

The following discussion in this submission seeks to provide some of this high-level advice at an early stage, to *"contribute to the design of this framework to deliver a real and meaningful uplift to critical infrastructure security and resilience, while minimising economic impact"*.

The coverage of this Submission follows a similar structure and discussion to the Consultation Paper.

It firstly focuses on AIP views on the objectives, coverage and scope of the 'Enhanced Regulatory Framework' (Section C). These views are set against the background of the key consultation question of 'where are we now' from a refining and fuels industry perspective in the following sections.

Specifically, Sections D, E & F provide general background information on the industry's internal and external operating environment and preparedness, in order to inform the appropriate application of the Framework to the sector and to also properly recognise the sector's existing challenges, circumstances and capabilities (an underpinning, and supported, Government objective emphasised in the Consultation Paper). This should also provide a starting point for the development of sector-specific guidance and standards where needed.

B. THE CURRENT REGULATORY FRAMEWORK

The *Security of Critical Infrastructure Act 2018* (the Act) came into force on 11 July 2018 and is *"designed to manage national security risks arising from foreign involvement in Australia's critical infrastructure in the electricity, gas, water and ports sectors."*

The Act aims to ensure that Government has all the necessary information to conduct national security risk assessments as well as the ability to enforce risk mitigations if they cannot be addressed through other means. It contains a range of obligations that apply in relation to specified critical infrastructure assets.

In particular, the Act introduced three key measures to address and manage these risks:

- a reporting obligation and asset register: entities who own and control assets must provide the Government with operational and ownership information
- an information gathering power: the Secretary of the Department of Home Affairs can obtain information and documents from reporting entities and operators in certain circumstances, and
- directions powers: the Minister for Home Affairs can intervene and issue directions in cases where there is a national security risk and mitigations cannot be implemented in collaboration with asset owners and operators.

Two types of entities are required to report under the Act:

- *A responsible entity*: the entity that holds or is otherwise declared to hold operational responsibility for the asset, and
- *A direct interest holder*: any entity (together with any associates of the entity) that holds at least a 10 per cent interest in the asset or holds an interest that allows the entity to directly or indirectly influence or control the asset.

The measures and obligations contained in the Act apply to both domestic and foreign owned critical infrastructure and take account of Australia's trade agreements and other international obligations.

The Act currently applies to *"the highest risk assets in the electricity, gas, water, and ports sectors where existing regulatory regimes are insufficient to manage these risks, or no other regulatory options are available".*

To date, the Act and its associated regulatory obligations have not been applied to the refining and downstream petroleum sector (i.e. to fuel). Rather, it has been applied to heavily regulated infrastructure and entities in the electricity, gas, water and port sectors – which are characterised as regulated monopoly infrastructure and high risk because they tend to represent "single points of failure" for ongoing economic and community activity.

Unlike these regulated sectors, the fuels sector operates in a highly competitive and diverse market with a different market structure and performance, and which has contingences and logistics flexibility (energy transport and storage) to help manage any supply disruption to one or multiple entities and facilities from any source. These features are described in more detail in Sections D & E.

C. ENHANCED REGULATORY FRAMEWORK: OBJECTIVES, COVERAGE & SCOPE

This Section provides AIP's high-level views on the key foundations of the 'Enhanced Regulatory Framework', being the objectives, coverage and scope of expanded regulations, including to a wider range of industries. These views are set against the fuel industry's current internal and external operating environment and circumstances, as outlined in Sections D, E and F. There is still much Framework detail to be developed and settled, and AIP and its member companies welcome further consultation on these aspects including to respond to many questions identified in the Consultation Paper and to fully assess the potential regulatory burdens imposed on businesses in the sector and the broader market impacts of the reforms.

OBJECTIVES AND CASE FOR REGULATORY EXPANSION

The Consultation Paper outlines an expansion of the 'current' regulatory framework noted above – called the 'Enhanced Regulatory Framework' - which will apply to a broader range of infrastructure assets, to the management of a broader range of threats to essential community services, and with an increase in the regulatory obligations on business entities involved in those industries covered by the Framework.

The Consultation Paper notes the primary objective of the proposed Enhanced Regulatory Framework is to*:*

- *"protect Australia's critical infrastructure from all hazards, including the dynamic and potentially catastrophic cascading threats enabled by cyber-attacks" and*

- *"uplift security and resilience in all critical infrastructure sectors, combined with better identification and sharing of threats in order to make Australia's critical infrastructure more resilient and secure."*

AIP member companies acknowledge that cyber security threats are persistent, evolving and increasingly severe, creating significant global challenges for governments and business to protect sensitive information, critical assets, the environment and the safety of the community.

It is important to protect key Australian infrastructure from national threats, including cyber attacks, where these are beyond the capability of individual entities and industries to manage themselves. That is, where a market failure or national security vulnerability exists or is demonstrated which could impact on the resilience of critical infrastructure, particularly facilities which represent a "single-point-of-failure" and thereby a vulnerability to the ongoing supply of essential services across Australia.

However, AIP notes that if government has national security objectives beyond the commercial imperatives and means of entities (including beyond current commercial approaches to working capital and facility, staff, operational and data security – see Section D) then appropriate government support should be provided to meet the additional costs of these government objectives.

AIP member companies do support the Australian Government taking action to protect private companies from cyber-attacks and providing strong deterrents against cyber-crime and nation state attacks. The issue then is what Government actions to take and their proposed scope and design.

The 'Enhanced Regulatory Framework' for Critical Infrastructure aims to "uplift resilience" of all critical infrastructure sectors through collaborative approaches and new government powers and a range of regulatory obligations, including applying these to a broader range of local industries.

The industry supports the government in taking the lead in improving Australia's situational awareness, as this will strengthen the cyber security posture and capabilities of each organization operating in Australia. The key to achieving this is proactively identifying and remediating cyber vulnerabilities via information and intelligence sharing between public and private sectors. Such actions are unlikely to create major imposts on business and would enhance threat assessments, planning and response from entities themselves.

The fuels industry actively participates in and values open and collaborative emergency management and information sharing on vulnerabilities between government entities and private partners, within legal parameters including competition law and data privacy legislation, to help prevent and manage threats. AIP members therefore welcome many Consultation Paper initiatives (on page 15 of Consultation Paper). However, AIP member companies support sharing of information on a voluntary basis, as opposed to mandatory disclosure, and full compliance with non-disclosure requirements unless agreed by entities.

Beyond information sharing, new regulatory imposts (rather than incentive based self-regulation and audits favoured by industry) remain a major concern to the industry operating in a competitive and challenging market environment and needing to deliver competitive consumer fuel prices (Section F). This is particularly the case where the government's regulatory role does not align with the industry's cyber and data privacy programs (Section D).

AIP also notes that the Enhanced Framework's objective of protection from 'all hazards' is an expansion of the original focus of the Act, which is currently focused on 'foreign involvement' in infrastructure assets. A strong case for this regulatory expansion into a much broader range of threats, and local business and market activity, has not yet been clearly made. The Consultation Paper simply suggests that threats are "significant", "increasing" and can have "flow on effects across multiple sectors".

There has also not been an opportunity yet to review exposure draft legislation supporting the Enhanced Framework, to assess whether the reforms are proportional to the risks and potential threats. AIP also notes that Economic modelling is being completed, in accordance with the Department of Prime Minister and Cabinet's Office of Best Practice Regulation guidelines, to ensure that *"these reforms are developed and implemented in a manner that secures appropriate outcomes without imposing unnecessary or disproportionate regulatory burdens".*

AIP and its member companies look forward to reviewing the exposure draft legislation, modelling and Regulatory Impact Statement when it is available.

In addition, the achievement of the stated Government objectives whilst also securing strong business support, will be critically dependent on the finer details of the Framework's design and application – including scope, specific obligations, relevant regulators, and how implemented for specific industries. The details of these fundamental dimensions are still to be settled and developed in consultation with key sectors including our industry. That is, the policy goals and general framework are clear, but the specific application, obligations and costs to industries are unknown at this stage.

The key balance to be struck in the Framework and its application is the extent to which *"driving an uplift in resilience across sectors"* is driven via regulatory approaches and obligations (with likely economic and business costs) rather than through collaborative approaches like the enhanced government-industry engagement, education and information sharing activities already proposed in the Consultation Paper.

The application of regulatory measures and costs on businesses would normally be supported by strong evidence confirming that such impacts are justified by a demonstrated higher level of risk currently and into the future, and that these risks are not already being effectively managed by specific sectors or entities. This case is also usually important to maintaining community support where higher service costs to consumers result from the imposition of new regulatory costs on business operations. Regular regulatory review is also included in most instances to ensure regulations meet their objectives and continue to be required in the prevailing environment.

The Consultation Paper also notes that the Framework (and obligations on infrastructure owners and operators) needs to recognise the wide range of differences and circumstances facing different sectors of the economy and be targeted appropriately (because *"one size does not fit all"*). As a result, it is proposed that the Framework will be *"built around principles-based obligations that will sit in legislation, and underpinned by sector-specific guidance and advice, proportionate to the risks and circumstances faced by each sector. Furthermore, legislative requirements will remain proportionate and collaborative, while avoiding inconsistent application of regulations putting entities at a commercial disadvantage".*

Where new sectors are brought under the scope of the Act and the Enhanced Framework for the first time, AIP member companies support the development of sector specific guidance and standards which are co-designed and collaborative and also proportionate to the risks and circumstances of different sectors and to the maturity of existing systems and standards (see Sections D and E). The policy principle of no commercial disadvantage in the application of any regulations is also strongly supported.

AIP member companies also welcome the Government's recognition in the Consultation Paper of *"the additional economic challenges facing many sectors and entities in the wake of the COVID-19 pandemic"* and the Government's commitment to industry to *"work in partnership to develop proportionate requirements that strike a balance between uplifting security, and ensuring businesses remain viable and services remain sustainable, accessible and affordable"; and "to deliver a real and meaningful uplift to critical infrastructure security and resilience, while minimising economic impacts".*

The current and ongoing economic challenges facing the refining and fuels industry, and the need to minimise industry cost burdens in this environment so the industry can remain internationally competitive and economically viable, is the main focus of Section F.

APPLICATION OF REGULATIONS TO AN EXPANDED SET OF INDUSTRIES

The Act currently applies to the highest risk assets in the electricity, gas, water, and ports sectors where existing regulatory regimes are insufficient to manage these risks, or no other regulatory options are available.

The Critical Infrastructure Resilience Strategy currently defines critical infrastructure as:

> *"those physical facilities, supply chains, information technologies and communication networks, which if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security."*

The Consultation Paper states that, within this definition, the Government proposes to introduce, under reforms to the existing legislation, proportionate obligations onto an expanded set of critical infrastructure sectors and assets - including the energy sector broadly defined.

The entities and critical infrastructure to be covered by the framework is a critical consideration. The cyber security laws and regulations applying globally are done so based on unique definitions and differences on what are considered 'Critical Infrastructure' (CI) in their respective countries (and based on each country's different national security and economic concerns and challenges).

Therefore, to ensure that an infrastructure is truly critical in Australia, AIP member companies support clear terminology and criteria/thresholds being developed for the appropriate identification of CIs in the proposed framework. In addition, where specific cybersecurity requirements apply to critical infrastructure, we support the use of clear terminology to ensure that only fuels related infrastructure that is truly critical, is treated as such.

In Government-Industry workshops conducted alongside the release of the Consultation Paper, it has been proposed that the Enhanced Framework and associated regulations will likely apply to all major facilities in the Downstream Petroleum Sector apart from retail operations. That is, to petroleum refineries, storage and terminal assets (including Joint User Hydrant Installations at airports), and distribution pipelines.

As noted above, the Act has not been applied to date to the refining and downstream petroleum sector (i.e. to fuel). It has been applied to regulated monopoly infrastructure and entities in the electricity, gas, water and port sectors, which have a different market structure and operational circumstances and management to the fuels sector (see Sections D & E) and which have a higher level of risk to their ongoing service provision in the event of disruption.

That is, while it is easy to understand the logic of how a major disruption to fuel supply could impact on national economic wellbeing and security, it is more difficult to identify the specific circumstances or threats that would compromise all the flexibilities, contingencies and response capabilities in the fuel supply chain, given the wide range of alternative supply sources, market entities, facilities and transport logistics needed to be compromised for a widespread and prolonged fuel shortage across Australia.

For example, Australian refineries are key infrastructure in the Australian market providing valuable supply diversity and flexibility, as well as supply security to the domestic market in addition to their significant economic benefits. However, in contrast to a supply disruption to an electricity generator for example, there are alternative fuel supply options that can be quickly called upon in the event of a refinery outage, as has occurred in the past.

These key market and operational differences necessitate a different, proportional and appropriately targeted approach by the Government to applying any new regulations on the fuels sector under the 'Enhanced Regulatory Framework', as the Consultation Paper states will occur.

This includes to ensure that regulatory decisions do not impose unjustified cost burdens on industry or undermine the competitiveness and viability of fuel refining and supply, particularly given the current challenges facing the industry (see Section F). This must be a prime focus for the next round of consultation on "proportionate sector-specific guidance and standards" which may apply to fuel and the relevant 'criteria and thresholds' determining what assets and entities within different segments of the fuel supply chain fall within the Act's scope and obligations.

REGULATORY OBLIGATIONS ON ENTITIES

Entities (infrastructure owners and operators) within the expanded set of critical infrastructure sectors under the Act, will have different obligations and elements of the Framework (regulatory coverage) applied to them depending on what 'class of entity' they are determined to be.

The classes of entities, in order of the range of obligations to be applied (from lowest to highest), include:
(1) *Whole of Economy* - entities outside the Act but covered by the 2020 Cyber Security Strategy
(2) *Critical Infrastructure Entities* - entities brought within an Expanded Act and subject to its directions and actions powers
(3) *Regulated Critical Infrastructure Entities* - brought into the Expanded Act and also incurring a 'Positive Security Obligation' to be enforced by an appropriate regulator to be determined.
(4) *Systems of National Significance* – the same obligations as Regulated Critical Infrastructure Entities but also including a range of Enhanced Cyber Security Obligations to "a small subset of entities.

The Consultation Paper indicates that criteria will be developed for assessing which entities will be covered by the reforms, and that these criteria will be guided by the principles of simplicity, transparency, accuracy and stability. It also states that the proposed reforms will be focused at the owner and operator level, not at a specific piece of technology to ensure interconnected assets are protected from cascading failures.

The Consultation Paper states that these criteria are to be developed on a sector-specific basis and taking into account the entities' external and internal operating environment. AIP member companies would welcome that consultation, particularly in light of our market circumstances noted in Sections D, E and F.

However, in Government-Industry workshops, it has been suggested that the entities owning, controlling or operating the downstream petroleum facilities proposed to be covered, would likely be classified as 'Regulated Critical Infrastructure Entities', to which the Positive Security Obligation would apply in addition to the current obligations under the Act. This would represent a new and major regulatory burden on the fuels industry (even if proportional and collaborative in design), as no regulation has previously applied.

POSITIVE SECURITY OBLIGATION

The Consultation Paper states that the *"Positive Security Obligation (PSO) will propose a set of principles-based outcomes across Australia's critical infrastructure sectors to protect entities from all-hazards"* and will apply to entities designated as 'Regulated Critical Infrastructure Entities' and owners and operators of 'Systems of National Significance'. The Paper also notes that Government wishes to work with industries to define the principles of the PSO, design the detail around how critical infrastructure entities in sectors can meet their PSO obligations, and also to identify the most appropriate regulator for each sector.

The proposed foundation principles of the PSO (minimum standard) is that *"owners and operators of critical infrastructure should be legally obliged to manage risks that may impact business continuity and Australia's economy, security and sovereignty, by meeting the following PSO* ***principles-based outcomes***":
- Identify and understand risks
- Mitigate risks to prevent incidents via proactive management
- Minimise the impact of realised incidents (on operations and customers)
- Effective risk management oversight, responsibilities and governance.

The proposed high-level **security obligations**, to be set out in legislation, are that regulated critical infrastructure entities will be required to:
- protect their systems and networks by considering and mitigating natural, and human induced threats
- protect their systems and information from cyber threats
- implement policies and procedures which seek to mitigate the risk of employees (insider threats) exploiting their legitimate access to an organisation's assets for unauthorised purposes
- protect their operations by understanding supply chain risk.

As outlined in Sections D and E, AIP member companies already systematically identify and manage risks and mitigate their impacts via robust and proactive planning, systems and governance approaches.

These measures are focused on business security and continuity of operations in accordance with their commercial, contractual and legal requirements, which underpin the entity's corporate and community reputation and licence to operate. While managing 'national security and sovereignty risks' are the domain of national governments, AIP members will support these national objectives by maintaining the security of their own facilities and operations and managing business risks and threats which they can control.

In principle, AIP member companies support incentivised self regulation and audits (encouraged through legislation) to demonstrate the adequacy of companies' security measures. In this regard, we also support and would participate in the development of risk-based industry guidelines and existing public-private frameworks to protect against cyber threats.

AIP members do not support, however, unnecessary mandatory or sanction-based security measures, which degrade (or disincentivise) ongoing cybersecurity investments by the industry and operators. This would occur where mandatory security measures or specific standards are imposed on individual AIP member companies despite being able to demonstrate that they have robust security measures and practices already established and there is a reasonable expectation of meeting security obligations.

RELEVANT REGULATORS, COMPLIANCE AND ENFORCEMENT OF SECTORS

Relevant regulators, to be designated by the Commonwealth, will monitor and enforce whether Regulated Entities are in compliance with these PSO outcomes and obligations. The Consultation Paper notes that the Government will work with critical infrastructure entities to identify the most appropriate regulator for each sector, recognising one size does not fit all and that there are various existing regulatory requirements for some sectors. These regulators will *"work with entities to co-design sector-specific requirements and guidance to ensure the PSO is applied, taking into account the needs and capabilities of each sector"*.

The choice of regulator for each sector will be critical. While the proposed regulatory model would avoid duplication with existing oversight requirements and specific industry regulators would normally be in the best position to provide guidance to entities on how to meet their obligation, the suggested compliance and enforcement process by the regulators seems to be overly administrative and once again raises concerns of degrading ongoing industry investments in cybersecurity.

AIP members companies do welcome the Government's commitment that:

- *"regulators will adopt a risk-based approach in developing and enforcing the PSO that emphasises education and guidance in the first instance"*
- *"Government considers that incident reporting, including actions taken to address those incidents, will be an essential component of this framework", and*
- *"Regulators should also consider the potential impact of PSO requirements and seek to minimise their economic and operational impact on businesses"*

However, AIP member companies do not yet have a clear view on the body who may be best placed to undertake the regulatory role broadly described, as the scope of the regulation and obligations applying to the sector is not yet confirmed and consulted on. As with all regulators, the industry would expect the relevant regulator to have the required expertise and resources, as well as strong industry understanding and links/networks, to undertake this security-related role in our specific sector, and whilst not duplicating other regulation and regulator activity (e.g. major hazard facility regulations which apply to many downstream petroleum assets). In addition, a regulatory and enforcement approach to the sector which is more heavily focused on industry resilience engagement and education might necessitate a different regulator to one responsible for compliance with the extensive 'enhanced cyber security obligations' for those entities' operating systems of national significance.

AIP notes that clear guidance and details of the compliance obligations, administrative arrangements and enforcement powers and approach are needed, as to be set out in the Act or the enabling legislation.

We note that the Consultation Paper suggests that the foundation of the compliance and enforcement approach will be an agreed Board-level (or equivalent) reporting submitted on an annual basis, and reporting against the PSO principles of risk identification and reporting. AIP member companies consider that any such reporting to the regulator should align with the existing business systems and reporting timetables of risk committees and annual reporting cycles within Entities, including to minimise regulatory imposts as the Consultation Paper commits to.

CYBER ASSISTANCE FOR ENTITIES

This initiative under the Enhanced Framework proposes actions, powers and protections in the event of critical infrastructure facing a significant cyber threat and the need to take active protective action in the national interest.

While the Government is relying on industry to take proactive steps to manage cyber security threats, there may be scenarios (impacting on Australia's economy security or sovereignty) that require Government intervention, specifically the ability of Government to intervene and issue directions in cases where there are significant national security concerns that cannot be addressed through other means.

In these cases, it is proposed that the Government will be *"able to provide reasonable, proportionate and time-sensitive directions to entities to ensure action is taken to minimise its impact"* and that *"entities may also be able to request that Government make such a direction, providing them with the legal authority to conduct any necessary action"*.

AIP member companies agree that companies must be empowered to take necessary, preventative and mitigating action against significant threats to protect their business, operations and the community. We also agree that government directions to entities may be needed in cases where companies do not have the legal authority for preventative or threat management actions because immunity is not provided under the terms of their current commercial contracts with other suppliers, customers and third parties. AIP members also support this level of Government assistance being provided on a voluntary (on-request) basis, as all entities should be well incentivised to expeditiously restore services and supply to their customers and the broader community.

The Enhanced Framework also anticipates that the Government can itself take 'direct action' or declare an emergency under legislation to protect or restore critical infrastructure and national systems, and where entities are refusing to do so themselves. While such actions in-principle appear in the National interest, significantly more detail and definition are required to understand the specific circumstances or scenarios where Government invention would be anticipated, on what terms, and following what process of engagement and notification.

Overall, AIP member companies fully understand that in times of national emergency there may be a need for government to intervene and issue directions or declarations to support response and recovery actions. However, in most cases, AIP member companies believe in taking their own proactive actions in responding to major cyber incidents and threats, and should be empowered to do so within the current and future legislative parameters and framework. Naturally the industry would seek Government assistance and be fully cooperative when necessary, but immediate direct intervention by the Government should be the last resort.

D. CURRENT INDUSTRY STEPS TO MAINTAIN PHYSICAL, CYBER AND PERSONNEL SECURITY

This section and Section E provide an overview of the key features and operation of the refining and downstream petroleum industry that are relevant to this consultation process – in particular, how operational risks and threats are proactively and expertly managed to ensure ongoing reliable supply of fuel across Australia. This industry overview, alongside the key challenges facing the industry outlined in Section F, is intended to guide the appropriate design and application of the 'Enhanced Regulatory Framework' to our sector and the development of sector-specific guidance and standards where necessary.

INDUSTRY STEPS TO MAINTAIN THE SECURITY OF FACILITIES, PERSONNEL AND DATA

AIP member companies have robust security measures and preparedness plans to protect their key facilities, personnel and data from a broad range of operational, physical and cyber security threats.

These plans and measures are risk-based, well developed and mature, and are benchmarked against leading Australian and global standards for security and risk management. They also seek to draw from global best practice methodologies, including through knowledge and technology transfers from international affiliates. They are also well supported within member companies by appropriate resources, operational technology and expert personnel.

This reflects how seriously these companies take all threats to the reliable and secure supply of fuel to their customers - the industry's core business objective at the forefront of all business continuity planning.

In many respects, physical and cyber security threats are viewed by the industry like other threats to reliable fuel supply to our customers which must be expertly managed (i.e. an 'all hazards' approach). These threats are addressed through orthodox risk management systems (see below) including robust business continuity planning, regular testing, and effective execution of counter measures when required. Equally important is ongoing staff training and education to support timely threat identification, avoidance and preparedness, and also their effective management when they materialise.

The security plans and programs of AIP member companies involve all these core elements and aim to be flexible to the different threats and environments where they operate throughout the domestic and global supply chains and also typically responsive to changes in the security environment over time.

These plans and programs are also regularly assessed and tested (including regular cyber threat testing and exercises during the year), including at localised and global operation levels, and also at individual facility levels under Facility Security Plans. The assessments by security personnel and experts are focused on continuously improving their capability in relation to threat assessment and management, and utilising the best risk management methodologies that may be available, including from various sources.

Education and awareness is also a cornerstone of each company's response to this threat environment, and there is regular cyber security training of staff and contractors to strengthen the early identification and response to cyber threats and to reinforce ongoing safe IT and workplace practices and behaviours. This is also a shared responsibility with business partners.

AIP member companies consider that these plans and programs are "fit for purpose for the modern age" (an objective noted in the Consultation Paper), based on each company's business risk assessments which draw from their own operational experiences and from the information available to them from various local and global business sources. However, these plans and programs are grounded in industry operation and 'business' risks, imperatives and intelligence, not 'national security' dimensions which are the domain of government.

AIP member companies recognise that neither business nor government, in isolation, have access to all the information needed to fully understand and mitigate risks to guarantee continuity of supply. It is also recognised that governments have unique capabilities to identify and address serious and sophisticated security and cyber threats to Australia, including through the national intelligence community, which is why government-industry information sharing and partnership approaches are particularly important.

It is also critical for the Government to fully recognise that regulated security standards and obligations are already imposed on AIP member companies and their facilities in various forms and at different points of their commercial operations and fuels supply chains. For example, amongst others, security and cyber obligations and conditions already exist as part of 'Major Hazard Facility' licensing conditions, 'Maritime Security Plans' for maritime facilities where we operate, State critical infrastructure legislation and requirements, and with Defence Industry Security Program (DISP) membership. AIP member companies consider that duplication of these regulated requirements should be strongly avoided under the Enhanced Framework, as the Consultation Paper commits to.

COLLABORATIVE GOVERNMENT-INDUSTRY INFORMATION SHARING

The ongoing maintenance of effective industry plans and programs to deal with physical and cyber security threats is highly dependent on a robust company and industry understanding of the threats and risks that they may encounter.

Availability of timely and high quality information on the latest security environment and threats enables plans and programs to be assessed, and recalibrated as necessary, to ensure they remain resilient to a broad range of potential threats and also able to manage imminent (known) threats.

The industry therefore places the highest value on voluntary and collaborative approaches between government and industry to information sharing (see Page 8) to improve and deepen the collective understanding of the threat and risk environment for the industry and other sectors we rely on.

As a result, AIP member companies strongly support the commitment in the Consultation Paper that *"Government should use its unique position and resources to share aggregated threat information, work with critical infrastructure entities of all levels of maturity to build their capability, and empower entities to appropriately protect themselves when faced with a serious threat."*

AIP and its member companies already routinely engage in a broad range of industry-government committees, standards development, training, exercises and forums aimed at maintaining the security and resilience of industry operations. This includes the Trusted Information Sharing Network for Critical Infrastructure Resilience (TISN) and a range of Commonwealth and State emergency management committees. The Consultation Paper notes that the Enhanced Regulatory Framework *"will be underpinned by enhancements to the Government's existing education, communication and engagement activities"*, and such initiatives would be welcomed by AIP member companies if they provide a strong value proposition by strengthening existing plans and programs within companies and the industry broadly defined.

E. CURRENT INDUSTRY STEPS TO MAINTAIN FUEL SUPPLY RELIABILITY AND SECURITY

This Section provides an overview of the fuel industry's effective and efficient management of fuel supply and supply chains, including managing risks and supply disruptions, to ensure ongoing reliable supply of this crucial service to communities, businesses and key Australian industries.

THE AUSTRALIAN FUELS SUPPLY CHAIN

Australia is well serviced by a resilient and diverse supply chain that delivers a high level of reliability by global standards, despite the significant challenges in distributing fuel across such a large country with a geographically dispersed population. The Australian supply chain includes crude oil and petroleum product shipments into and around Australia, refinery throughput, bulk fuel storage tanks, extensive terminal, storage and distribution networks, around 7000+ retail outlets, and fuel storage facilities of major users.

The fuel supply chain works to match Australian fuel demand and quality specifications, including in different Australian jurisdictions, with international and domestic refinery capabilities. There are strong business pressures on refiners and fuel suppliers to maintain a resilient and efficient supply chain, since this is essential for reliable supply and meeting customer expectations.

The Australian fuel supply chain and associated infrastructure has been independently assessed as being secure and functioning efficiently and effectively to meet Australia's current and future fuel supply needs. This performance is underpinned by considerable industry investment in new and expanded supply infrastructure, and a requirement for significant ongoing investment to maintain the existing capacity.

The risks associated with these investments are minimised through long term supply contracts with suppliers, major fuel users and customers.

There are vital commercial incentives for efficient infrastructure and supply chain management including:

- maximum utilisation of infrastructure (including via hosting and joint venture arrangements)
- an ongoing program of infrastructure maintenance
- holding fuel stocks which reflect a robust commercial assessment of demand, operational conditions and risks in each location
- regular review of supply chain operations and infrastructure adequacy.

Regular reviews by the industry have led to the construction of new or expanded supply infrastructure and fuel storage in key import and demand centres around Australia, to better meet changes in the customer base and the fuel products they require.

Within this supply chain, diversification of supply sources is one of the most important elements of liquid fuel supply security. Diversity of supply avoids over-reliance on any single supply source and helps mitigate risks from potential supply disruptions.

Australia has a high level of supply diversity built into its fuel supply chain including multiple supply networks into Australia, a number of domestic refineries, multiple and flexible import and distribution networks in each State/Territory, and a range of alternative fuel suppliers and importers throughout the supply chain. This means that fuel can be delivered in a number of ways to where it is needed, during normal operations and also during supply disruptions or other emergency situations.

Australia's liquid fuel supply security risks are spread between imported crudes and products from a variety of different sources (40+ sources for imported crude oil and 66+ sources for imported products) and domestic crudes and products from a variety of different sources.

Australia's capacity to process crude oil in domestic refineries, including local crude, provides additional supply diversification and flexibility, underpinning Australia's supply security.

Also, over the last decade the growing volume and frequency of petroleum products imported into Australia have increased domestic supply reliability. According to the official statistics (APS), about 2-3 weeks of supply owned by Australian companies is typically on the water at any time, with a large proportion of this stock in Australian waters. This is some 30 per cent of all stock owned by AIP member companies.

The significant volume and wide distribution of cargoes of crude oil and petroleum products on the water serves as a form of floating storage which provides a diverse and flexible source of supply. It also provides an efficient and cost effective logistical and storage solution, which is now fundamental to managing ongoing reliable supply of liquid fuels to Australian markets and customers. The highest level of fuel supply flexibility and reliability is achieved when stock on water can be readily diverted between Australian locations on an as needs basis.

Australia's access to diverse supply sources and well-established international and domestic supply networks suggests that any future disruption risks are unlikely to compromise Australia's access to the physical supply of liquid fuels.

INDUSTRY MANAGEMENT OF SUPPLY AND SUPPLY DISRUPTIONS

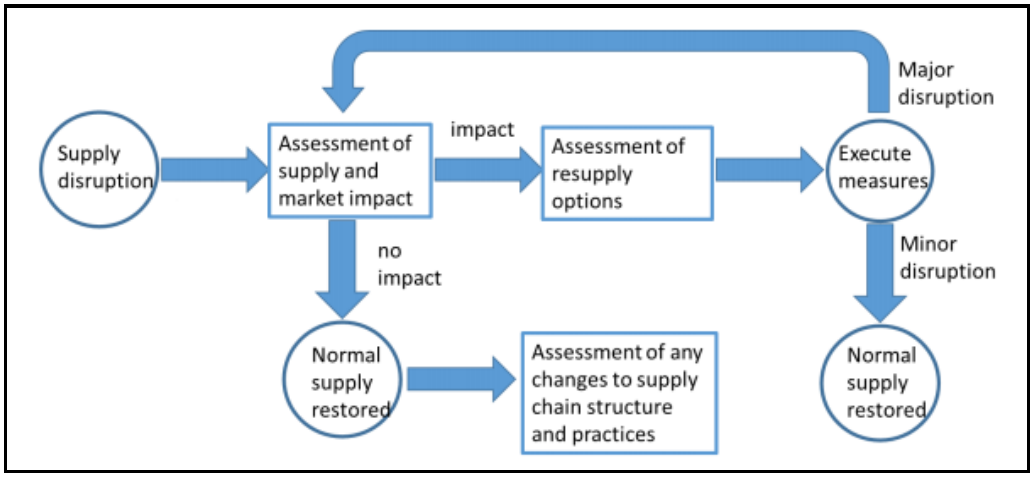
AIP members seek to ensure continuous and reliable supply of fuel to all customers and areas of Australia, which involves simultaneously managing all aspects of the supply chain. Industry considers reliable supply of high-quality fuel essential to maintain customer brand loyalty, as well as to maximise business commercial viability.

Nonetheless, unplanned events can create fuel supply challenges at short notice including unplanned refinery disruptions, breakdowns in key supply infrastructure or pipelines, delays in ship arrivals, natural disasters, and customer demand exceeding contracted supply requirements.

Each supply disruption develops in its own way and requires dynamic industry management. Almost all supply problems are capable of being managed by industry and the market.

However, there are also well-established arrangements for relevant Ministers and departmental officials to be kept fully informed of developments when there are emerging issues or actual supply disruptions so that governments are well positioned to assist with supply management if needed.

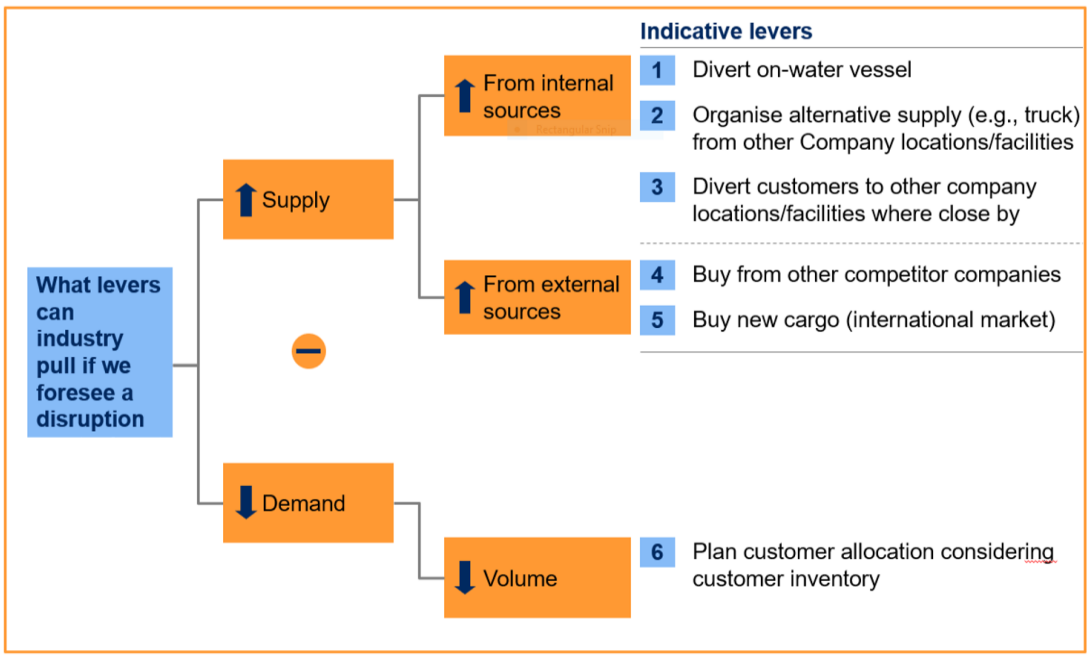
As the management of reliable fuel supply is the industry's core commercial business, there is constant monitoring and review by fuel suppliers of supply chains, customer demand, commercial stockholdings and bulk fuel transfers/shipping in every location. As a result, a disruption event which impacts or is likely to impact the supply chain or reliability will set off a reasonably orthodox organisational management approach to managing risk – as illustrated in the chart below. The fuels industry is no different from other industries in that regard, except its responses will take place within the timeframes to which the fuels industry operates.



Industry has rapid and comprehensive response strategies in place to replace any lost supply. These strategies include:

- numerous technical options within refineries
- utilising alternative supply infrastructure and supply and distribution routes
- sourcing supplies from other Australian refiners and/or fuel wholesalers
- sourcing supplies from international sources and the spot market
- redirecting product already on route to Australia to the impacted location
- equitably allocating bulk fuel to customers
- drawing down industry stockholdings.

Industry response strategies, in simple terms, are illustrated in the chart below.



Given the wide range of logistical options and contingencies, the management of fuel supply disruptions is dynamic to respond to specific market circumstances at the time, which is more targeted and valuable. As this is part of normal day-to-day industry operational processes, it is not handled like emergency situations in the electricity and gas sectors, and even very serious fuel supply disruptions are handled in a similar way to moderate disruptions (but would typically involve a broader range of response options, internal parties and external stakeholders).

The flexibility of the fuels supply chain to respond to specific events or circumstances also greatly assists the management of emergencies outside of the industry's direct control (e.g. other energy sectors, extreme weather events). For example, the petroleum industry provided good support and diesel supply to other energy sectors experiencing problems such as the Varanus Island gas explosion and the Tasmanian electricity disruption.

Industry is confident in its supply management and the commercial stockholdings held and has a very longstanding reputation for reliably and safely meeting their customers' demands. This confidence is demonstrated by the fact there has been no widespread or sustained fuel shortage for decades in Australia (including during major global disruptions and wars like the US Hurricanes, Global Financial Crisis, Iraq War, Kuwait invasion, and Libya crisis).

In this context, AIP members believe that the most appropriate action for dealing with all but the most serious supply disruption is for the market to be allowed to operate with minimal government intervention.

This view is supported in a range of Government reports, and in the Liquid Fuels Emergency (LFE) Act and National Liquid Fuels Emergency Response Plan (NLFERP) and in the Emergency Plans at a jurisdictional level which all consistently advise *"disruptions are largely managed by industry, and government intervention is a last resort".*

While current industry response strategies are highly effective, these could be further enhanced by the more widespread adoption of active supply management and business continuity planning by major fuel users supporting the economy.

THE FUELS SECTOR IS VERY DIFFERENT TO OTHER ENERGY SECTORS

The economic and operational differences between the fuels sector and other energy sectors – in terms of market structure, conduct and performance and also its response to supply disruptions – has for a long time necessitated a very different policy and regulatory approach by Government to the fuel market.

This is underscored by the features and operation of the fuels market detailed above – particularly the supply diversity, logistics flexibility (energy transport and storage) and supply contingences in the event of disruption, as well as rigorous market competition to supply the end-user – which contrast strongly with other energy sectors, particularly electricity.

For example, the fuels market and the electricity sector are two totally separate and largely unrelated forms of energy, that have totally different markets in terms of their structure, conduct, price response and performance/operation, including in the event of a supply disruption. Whilst most of the electricity sector can be considered as a national supply chain with significant interconnectedness across states and geographic regions, the liquid fuels market is not interconnected in the same way.

Petroleum is a primary energy source and is the largest globally traded commodity with extensive supply diversity and market operators and participants – both globally and domestically. It is a 'genuine market' with market determined prices and intense competition to supply the fuel that local consumers and business demand. Electricity is a secondary energy source focused domestically with regulated monopoly infrastructure and with limited market suppliers and alternatives in the event of a supply disruption.

The performance of the fuels sectors in delivering reliable and affordable energy over the many decades stands in stark contrast to the electricity sector.

ROBUST GOVERNMENT-INDUSTRY EMERGENCY MANAGEMENT ARRANGEMENTS

In the case of the liquid fuels market, industry and governments recognise the potential risks and impacts of a disruption to liquid fuel supplies. AIP and its member companies actively participate in government sponsored emergency management committees like the National Oil Supplies Emergency Committee (NOSEC).

While every effort is made by industry to ensure continuing reliable supply, the International Energy Agency (IEA), NOSEC and State emergency management committees have established emergency response plans that would help ensure a coordinated response to any major fuel supply disruption or oil emergency at an international, national or jurisdictional level – including from any source including physical security and cyber threats.

AIP considers that Australia has a robust 'Emergency Response' framework and emergency management plans for liquid fuels which are consistent with Australian market characteristics, utilises established and tested industry commercial practices, and adopt those best practice IEA practices that will be effective in our specific market circumstances.

These plans are routinely tested through exercises and are regularly reviewed in accordance with legislative requirements and government objectives. An upcoming review of the Liquid Fuels Emergency Act has been announced by the Government and the industry will actively participate in this review.

F. CURRENT ECONOMIC CHALLENGES FACING THE REFINING AND FUELS INDUSTRY

AIP member companies welcome the Government's recognition in the Consultation Paper of *"the additional economic challenges facing many sectors and entities in the wake of the COVID-19 pandemic"* and the Government's commitment to industry to *"work in partnership to develop proportionate requirements that strike a balance between uplifting security and ensuring businesses remain viable and services remain sustainable, accessible and affordable"; and "to deliver a real and meaningful uplift to critical infrastructure security and resilience, while minimising economic impacts".*

This commitment is crucial in the context of the very significant economic challenges, and viability threats, currently facing the industry. This Section outlines these economic challenges facing the Australian refining and fuels industry, including ongoing competitive pressure from Mega refineries in Asia, the major financial and demand impacts of COVID-19, and the current unsupportive market outlook which is forcing a reassessment of the long-term viability of local and global refineries (particularly in the context of the requirement for major ongoing capital expenditure on refineries to maintain safe and reliable operations).

This market background is intended to guide the appropriate application of the 'Enhanced Regulatory Framework' to the downstream petroleum industry, and to ensure careful consideration of any new imposts and costs imposed on the sector which may not be justified or which could undermine the competitiveness and viability of the refining industry.

ONGOING ECONOMIC CHALLENGES FROM ASIAN MEGA REFINERIES

Australia has four oil refineries that produce around half of Australia's total transport fuel requirements and a range of specialty products. These refineries provide a range of direct and indirect economic benefits to Australians and the Australian economy, and support supply security for liquid fuels.

The refining and fuel supply industry is capital intensive, and requires significant ongoing investment to operate safely and reliably. This investment occurs in a highly competitive and truly global market, where capital is deployed to its best use and highest return in terms of financial and operational performance benefits to companies.

The capital investment programs of Australian market operators have been challenged for some time by excess supply capacity in Asia, and increased competition from mega-refineries in Asia.

Australian refineries have to vigorously compete with newer Asian refineries that benefit from a number of competitive advantages, including:

- economies of scale - with larger production runs, lower capital and labour costs per unit of production, and the ability to purchase crude feedstock in large quantities at lower unit costs
- the latest technologies - with efficiencies released from greater flexibility in the crude oil inputs and product slate produced
- lower construction and labour costs for new and expanded refinery investments
- attractive taxation and investment regimes and allowances.

The competitive disadvantages for Australian operators compared to Asia can impact adversely on the decisions that must be taken locally on investments in major refinery, facility and supply chain upgrades and increased capacity. In essence, alternative supplies and operational capacity can be funded or readily sourced from the Asian region. This is the cause for some local refinery closures in the past.

In addition, overlapping federal, state and local government regulations locally also pose significant constraints on new investment in Australia and increase the complexity of operations and raise the costs of doing business in Australia.

Refineries have sought to manage the ongoing competitive and viability challenges themselves by improving the efficiency of their operations through enhanced refinery yields, high utilisation rates and operational reliability, and ongoing programs in all refineries of stringent cost containment.

Governments also have an important role in supporting considerable industry efforts to meet these challenges. Namely, in ensuring that future regulatory decisions do not impose burdens on industry or undermine the competitiveness of domestic fuel refining and supply and in carefully reviewing and streamlining existing complex and overlapping regulatory measures to ensure that current measures are soundly based and cost effective.

Notwithstanding these ongoing challenges, investment in Australian refineries and supply infrastructure has continued to occur over the last decade, and there has been confidence in the outlook for the industry. As noted earlier, over the last decade, AIP member companies have invested billions of dollars to maintain the reliability and efficiency of fuel supply meeting Australian quality standards.

However, in more recent years, these industry initiatives and investments have not been well supported by a strong and positive market environment, with an extended period of low refiner margins. This environment and outlook have further deteriorated with the unprecedented impacts of COVID-19 on the global and domestic oil and fuels markets, and on global economies more broadly, which are not expected to be short lived.

IMPACTS OF THE COVID-19 PANDEMIC ON THE REFINING AND FUELS INDUSTRY

COVID-19 has had significant impacts on global and domestic markets including falling oil and fuel prices, a major deterioration in refining margins, unprecedented falls in oil and fuel demand globally and in Australia, refineries locally and across the globe scaling back production or bringing forward essential maintenance, and regional and global oil storage being under pressure to hold excess crude and product (e.g. Jet) inventories until refinery and consumer demand recovers.

In early 2020, the onset of the COVID19 Pandemic created an unprecedented set of market conditions and associated operational challenges for the Australian industry, including substantive demand destruction for petroleum products (including a 50% fall in gasoline demand and an 80-90% decline in jet fuel demand at the peak of restrictions). As a consequence, refinery production dropped to its lowest level on record and some AIP member companies have already reported to the market the significant financial losses associated with refinery operations over the past year.

Many of the short-term operational challenges were able to be addressed, including through changes in fuel quality specifications with assistance from Government to provide some assistance in managing excess jet fuel inventories.

However, more concerning is the short-to medium term financial ramifications of COVID19, with refiner margins currently, and forecast to remain, unsustainably low into the future. Fuel demand is directly correlated to economic growth, and as a consequence of COVID19, economic growth is predicted to be significantly lower with commensurate reductions in petroleum demand.

In turn, previous confidence in the outlook on investment in refineries has been heavily eroded, not only within Australia but globally. Refineries are now reassessing their long-term viability with structural adjustment in the industry inevitable.

Further exacerbating the challenge for Australian refining is the regulated change to low sulfur gasoline by 1 July 2027. The capital investment required to produce gasoline to meet the new fuel standard had already presented a significant challenge for Australian refineries but has now been further compounded due to the outlook arising from COVID19. The move to 10ppm gasoline across all petrol grades is expected to require a capital spend of around $1bn across the four Australian refineries, along with significant additional operational expenditure, with no additional production or commercial benefits accruing to operators.

The funding of these extensive capital expenditure programs will be seriously challenged by shareholders and capital committees given the limited returns expected over the short to medium term. This outlook reflects the forecast persistence of the negative impacts of the COVID-19 Pandemic on economic growth and fuel demand locally, regionally and globally, and the consequences for the regional supply-demand balance and refiner margin outlook.

As a result, there remain significant uncertainties related to the pandemic's ongoing impacts on international and domestic fuels markets and on refinery operations. For example, the pandemic continues to have a significant impact on the Australian refineries, including their manufacturing operations, major maintenance activity and ongoing economic viability. As a result, the Australian Government is currently working with the refining sector, and has made announcements recently that were welcomed by industry, in full recognition of these economic impacts on local refineries.

6. NEXT STEPS

AIP and its member companies look forward to further consultations with Government on the Enhanced Regulatory Framework, and welcome many of the starting-point principles, consultation and impact minimisation commitments made in the Consultation Paper.

There is still much detail surrounding the Framework to be developed and settled, including the development and "*co-design of sector-specific requirements and guidance to ensure the PSO is applied, taking into account the needs and capabilities of each sector*".

AIP and its member companies welcome further engagement on these aspects including to respond to specific questions identified in the Consultation Paper on a more informed basis, and to fully assess the regulatory burdens imposed on businesses in the sector and the market impacts of reforms more broadly.

AIP is happy to discuss any aspect of this submission with Government stakeholders – please contact Nathan Dickens, Deputy CEO AIP, on [redacted].

AIP is happy for this submission to be made publicly available.