[redacted]
[redacted]
Critical Infrastructure Centre
Department of Home Affairs

Email: ci.reforms@homeaffairs.gov.au

Dear [redacted]

AIP SUBMISSION ON THE EXPOSURE DRAFT SECURITY LEGISLATION AMENDMENT (CRITICAL INFRASTRUCTURE) BILL 2020

The Australian Institute of Petroleum (AIP) welcomes the opportunity to provide a submission to this consultation process on the Exposure Draft of the *Security Legislation Amendment (Critical Infrastructure) Bill 2020* and explanatory documents.

This Submission is made by AIP on behalf of its four core member companies – Ampol Limited, BP Australia Pty Ltd, Mobil Oil Australia Pty Ltd and Viva Energy Australia Pty Ltd. These companies operate all 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 and distribution and retail networks.

We appreciate the engagement with AIP to date by the Department of Home Affairs on the development of an 'Enhanced Framework' to underpin the security and resilience of critical infrastructure, whilst minimising the potential for business and economic impacts from these new regulations and activity.

AIP member companies 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, design and business imposts of these Government actions.

AIP's previous Submission on Consultation Paper ('Protecting Critical Infrastructure and Systems of National Significance') provided detailed information on the industry's internal and external operating environment and preparedness, in order to inform the appropriate application of the Framework to the fuels sector and to also properly recognise the sector's existing significant challenges, circumstances and capabilities (an underpinning, and supported, Government objective emphasised in the Consultation Paper).

The industry supports the government in taking the lead in improving Australia's situational awareness, as this will strengthen the cyber security 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 collaborative and voluntary 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.

Beyond information sharing, new regulatory imposts remain a major concern to the industry operating in a competitive market and needing to deliver competitive consumer fuel prices. Concerns about regulatory imposts are also magnified in the current environment – given ongoing financial impacts of COVID-19, the negative outlook for the local and global refining industry, and the Government's clear recognition of these impacts in announcements and ongoing consultations with industry on the Fuel Security Package to address the ongoing viability challenges faced by Australian refineries.

In this environment, AIP member companies welcome the clear Government commitments in consultations to date 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".*

In principle, the Exposure Draft legislation and explanatory documents appear to strike that balance, by proposing to apply the Positive Security Obligation (PSO) to the fuels sector. AIP member companies support incentive based self-regulation (encouraged through legislation) to demonstrate the adequacy of companies' security measures, and also support the development of risk-based industry guidelines and existing public-private frameworks to protect against cyber threats.

However, there is much detail still to be developed and finalised, particularly for industry to be satisfied that these Framework objectives will be delivered in practice without unintended impacts and business costs. AIP member companies therefore welcome the commitment to consult closely with the fuels sector next year in the development of the "Rules" and other sector specific arrangements to apply to fuels, and to the proposed RIS process to demonstrate a net community benefit from these obligations.

The entities and specific critical fuels infrastructure to be covered by the framework and PSO is a key consideration. While refineries, pipelines and storage assets are within scope of the draft legislation, it will be important to ensure that only infrastructure assets that are truly critical in Australia are treated as such. This can be achieved, in consultation with industry, by the development and application of clear definitions and thresholds which are relevant to Australia's security, economic and fuels market circumstances.

For fuels infrastructure 'specified' in the Rules as critical under agreed terminology, the next considerations are which of the PSO requirements will apply to these assets and entities, and what is the most efficient regulator and compliance and enforcement approach to reduce administrative burdens. Another key area for consideration is how existing State-based regulatory and administrative requirements for critical infrastructure could be integrated into the Framework to ensure administrative efforts are not duplicated.

In all future consultations, AIP member companies will continue to seek collaborative approaches which:

- are proportionate to the risks of the fuels sector and to the maturity of existing systems and standards
- do not degrade (or disincentivise) ongoing cybersecurity investments by market operators
- align with industry's existing risk management and reporting, and cyber and data privacy programs
- avoid the inconsistent application of regulations which places entities or specific assets at a commercial disadvantage (as the Government has committed to do).

In addition, if the Government has national security objectives beyond current commercial imperatives (to protect infrastructure, operations, working capital, staff and data), then government support should be provided to address any major cost imposts on business from these government imperatives.

AIP and its member companies look forward to further consultations with the Home Affairs Department on the sector-specific rules and PSO requirements to apply to fuels. AIP is happy to discuss any aspect of this Submission with Government stakeholders and for this submission to be made publicly available.

Yours faithfully

Nathan Dickens
Deputy CEO

26 November 2020