AGL Energy Limited
T 02 9921 2999
F 02 9921 2552
agl.com.au
ABN: 74 115 061 375

Level 24, 200 George St
Sydney NSW 2000
Locked Bag 1837
St Leonards NSW 2065

Department of Home Affairs

Submitted via email: ci.reforms@homeaffairs.gov.au

16 September 2020

Dear Sir/Madam,

AGL Energy (AGL) welcomes the opportunity to make a submission in response to the consultation paper on Protecting Critical Infrastructure and Systems of National Significance (Consultation Paper).

AGL is one of Australia's largest integrated energy companies and the largest ASX listed owner, operator, and developer of renewable generation in Australia. AGL is committed to meeting the needs of its energy customers through our diverse power generation portfolio including base, peaking and intermediate generation plants, spread across traditional thermal generation as well as an array of renewable sources. AGL is also a significant retailer of energy and provides energy and telecommunications solutions to over 3.95 million customers in New South Wales, Victoria, Queensland, Western Australia, and South Australia

AGL supports measures to improve the security and resilience of critical infrastructure, and the focus on industry led specific measures and understandings, and collaborative relationships, instead of interventionist action.

AGL recommends that the use of designated legislation similar to that being employed in the Consumer Data Right program would be more appropriate for these broad reaching reforms. It will enable the Department to draft and the Government to enact the overarching principles in legislation this year, but a sector would need to be designated by the relevant Minister to draft and enact the relevant regulations and responsibilities.

This would allow proper consultation on who the proper authorities should be, the thresholds for application of these reforms, the costs of the reforms and various other aspects that require more detail and time for consultation to identify and mitigate any unintended consequences. Particularly as these reforms have the potential to considerably change the way asset owners' structure and manage their business, the wide breadth of sectors likely to be affected by these reforms and the implementation pathway considering the effects and resource constraints imposed by the current COVID-19 pandemic.

Given the limited Federal Parliament sitting days in the second half of 2020 and the proposed short tight timeframe set by Government for these reforms, AGL recommend that the consultation time be extended and that an additional stage with adequate time for consultation with relevant stakeholders will be required including a Draft Report and a Draft Exposure Bill. Furthermore, once the legislation has passed and the obligations are clear there should be adequate timing to become compliant with any regulations and obligations as many will involve a considerable uplift in processes, programs and systems for entities.

Multi-service entities:

It is pleasing that the Department has envisaged the framework as proposed to 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.

However, as society moves towards an increasingly digital world there are many asset owners, corporates and businesses that increasingly offer a variety of services to their customers that straddle more than one industry. AGL currently offers electricity, gas, broadband and mobile services, electric vehicle subscription service including the rental of the vehicle itself, residential and commercial batteries and solar panels.

Under the proposed reforms the provision of these services would be subject to sector-specific requirements and guidance to ensure the Positive Security Obligation (PSO), is applied appropriately. AGL requests that multi-service providers are considered in these discussions and that there is collaboration across the respective regulators. For example, the issuing of security notices and the provision of detailed guidance on how to achieve compliance. For cybersecurity and supply chain obligations it is very difficult to comply with two different and possibly conflicting industry standards and reporting obligations for a piece of software employed across the entire company.

In addition, the increasing prevalence of digital connectivity through the Internet of Things (IoT) and the emergence of two-sided markets, the challenge of defining the boundary line between critical and non-critical infrastructure owners and their and systems requires adequate consideration.

Government-Critical Infrastructure collaboration to support uplift:

AGL welcomes the proposal to enhance the Government's existing critical infrastructure education, communication, and engagement activities, through a reinvigorated TISN and updated Critical Infrastructure Resilience Strategy.

Specifically, AGL would like to see improvements in the sharing of information from the Government to entities like AGL that have submitted information under various requests and registration processes. Currently AGL is unable to retrieve copies of registrations or otherwise access information submitted to the Register of Critical Infrastructure Assets which complicates record keeping and audit processes. AGL recommends that reporting entities be able to access information they have reported to the Critical Infrastructure Centre and/or on the Register of Critical Infrastructure Assets.

In addition, it is vitally important that this uplift focusses on two way communication between owners/entities/assets and the various Government Departments including the Department of Foreign Affairs, Treasury and other relevant agencies to ensure co-ordination for messaging and management of any threats or hazards.

Initiative 1: Positive security obligations (PSO) – Principles-based outcomes, Security obligations and Regulators:

The PSO is broad in terms of the obligations likely to be placed on asset owners and entities, AGL hopes that the legislation is drafted in a manner that assigns obligations and responsibilities that are practical, realistic and involve two-way communications with the relevant Government bodies.

As mentioned earlier in the paper AGL suggests that the creation of any new security obligations should only occur:

- after a thorough assessment of issues and underlying causes that the obligation is seeking to specifically address;
- consideration and potentially adoption of existing regimes and processes including voluntary actions. In the energy sector, the Australian Energy Market Operator (AEMO) has established an Energy Sector Cyber Security framework. AGL believes the work that has gone into this should form the basis of the energy sector obligations under this Consultation. The framework has been developed

through industry consultation and is based on industry self-attesting their Cyber maturity against the framework. The AEMO framework is based on criticality and is being expanded to address emerging energy transition, including Distributed Energy Resources, large scale batteries and gas;
- consideration of options to address those outstanding issues and causes;
- After understanding and not unintentionally stranding investments industry participants have undertaken to protect critical infrastructure. For example, AGL is investing financial and human resources to uplift Cyber Security processes and maturity; and
- The proper cost-benefit assessments of such obligations.

This will be key in avoiding the duplication that the Department has mentioned it is keen to avoid.

The creation of new requirements and obligations for sectors particularly for procurement/supply chain and cybersecurity that are not historically subject to the critical infrastructure security regime may create issues for contracting as there may be a disproportionate regulatory burden for those businesses and they will no longer engage with business' that are subject to the critical infrastructure legislation. Specifically, with regard to information technology contracts, many providers including monitoring services are offshore and there may be limitation to which the entity/owner can share information or request information from that provider.

Similarly, any information requests issued to entities should only be issued if the information has not already been provided to either the regulator or another Government Department. The energy industry is subject to significant and multi government agency information requests and this often results in duplication of effort to answer regulatory notices or requests for information from different departments or regulators when that information has already been provided in a prior notice or RFI. Communication and co-ordination amongst departments and regulators for information requests would assist both the entities and the Government to produce and receive information in a timely manner.

For AGL to provide a fulsome commentary and analysis of the potential cost impact will require further detail on the proposed requirements and actions before this can be properly answered.

Initiative 2: Enhanced cyber security obligations – Situational awareness and Participation in preparatory activities:

AGL supports collaboration with Government on the enhanced cyber security obligations but notes that this type of engagement would require guidelines and safeguards to encourage the open flow of information. Further considerations should include:

- Immunity during the provision of live threat/hazard information. The real-time provision of this information may be subject to inaccuracies depending on the nature and scale of the threat;
- Understanding of what constitutes a threat, hazard, levels of severity. Qualitative data on events that have occurred and benchmarking of behaviours;
- The technical methods of information sharing should not create additional security concerns; and
- The actionable and timely sharing of information.

Initiative 3: Cyber assistance for entities – Establish the capability to disrupt and respond to threats:

This proposal requires further clarification and development as it affects the independence and autonomy of private businesses. Although the power for the Minister to intervene is already captured in the *Security of Critical Infrastructure Act 2018* (Cth) and contains a wide Ministerial directions power to direct owners and operators of certain critical infrastructure, the requirements under this third initiative extends to additional industries and assets and requires careful and detailed consideration of impacts/unintended consequences, mitigations and safeguards.

Particularly with regard to the legal responsibility for actions taken by the Government in circumstances where they either direct an entity or act on behalf of one and there are adverse consequences. Once again in order for AGL to provide a fulsome commentary and analysis of the potential cost impact will require further detail on the proposed requirements and actions before this can be properly answered.

AGL welcomes the opportunity to work closely with the Department of Home Affairs as the consultation and the legislative development progresses. In the attachment we provide responses against the specific questions raised in the consultation paper.

If you would like to discuss any aspects of our response further please contact Marika Suszko, acting Regulatory Strategy Manager, msuszko@agl.com.au.

Yours sincerely,

Elizabeth Molyneux

General Manager, Policy and Market Regulation