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, [redacted].

Yours sincerely,

Elizabeth Molyneux

General Manager, Policy and Market Regulation

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

Attachment 1: AGL response to questions posed in the Protecting Critical Infrastructure and Systems of National Significance Consultation paper:

Question	Question	AGL Response
2	Do you think the current definition of Critical Infrastructure is still fit for purpose?	Thresholds will be required to ensure that not every entity that is involved in the generation, storage and transmission of electricity or gas is captured. Small wind farms for example should not be subject to the same regulations as large coal fire assets. A threshold of scheduled generation for example may be used to exclude smaller assets whose output could not be considered critical to the security of the energy market.
4	What are the common threats you routinely prepare for and those you have faced/experienced as a business?	AGL would direct the Department to the All Hazards framework for the most common threats considered by critical infrastructure owners and operators.
5	How should criticality be assessed to ensure the most important entities are covered by the framework?	As a starting point criticality should be based on the criticality of the services provided to the market or consumers.
6	Which entities would you expect to be owners and operators of systems of national significance?	Any organisation that has the ability to significantly disrupt an essential service to be part of the systems of national significance. This would also include a look at the dependencies management across multiple industries and entities to look holistically at a system.
9	How else should government support critical infrastructure entities to effectively understand and manage risks, particularly in relation to cross sector dependencies? What specific activities should be the focus?	Government should provide clear guidance to ensure consistent application of entity self-assessments including aiding the identification of cross industry risks. This may include providing guidance on baseline industry risks (i.e. risks that apply to all entities); and targets for mitigation particularly as the consultation proposes that entities may be legally obliged to manage risks.
10	Are the principles sufficiently broad to consider all aspects of security risk across sectors you are familiar with?	For cybersecurity, particularly the enhanced obligations, the obligations should focus on understanding threats that are relevant to the organisation, monitoring threats as they evolve, estimating likelihood of materialisation and associated impact. Understanding the effectiveness of the related preventative and reactive controls through review and testing is important as this covers both information protection and system continuity, which seem to be the outcome the government is seeking. The definition of hazard does need to be considered and well defined in order for the principles around hazard identification and risk management to be realistic. Risk management is not about

		eliminating all risk so entities should not be required to prepare all hazards that may exist.
13	What costs would organisations take on to meet these new obligations?	Further detail on the obligations is required in order to undertake an assessment of costs.
14	Are any sectors currently subject to a security obligation in-line with these principles? If so, what are the costs associated with meeting this obligation? Does this obligation meet all principles, or are enhancements required? If so, what?	AEMO is implementing an energy sector Cyber Security Framework (AESCSF) which covers the obligations, in a more comprehensive manner.
15	Would the proposed regulatory model avoid duplication with existing oversight requirements?	Further detail is required to understand how regulators across industries will co-ordinate to regulate entities that offer a variety of services across multiple industries. However as noted above AEMO has already performed a considerable amount of work into the Cyber Security Framework and this should be the basis for any cybersecurity obligations under the reforms.
16	The sector regulator will provide guidance to entities on how to meet their obligation. Are there particular things you would like to see included in this guidance, or broader communication and engagement strategies of the regulator?	Further detail is required to answer this question including who the sector regulator would be.
18	What kind of support would be beneficial for sector regulators to understand their additional responsibilities as regulators?	Support to ensure alignment across sectors. As companies are expanding across multiple sectors the sector specific standards may create an administrative burden where inconsistencies will add significant time and cost to the process of compliance.
19	How can Government better support critical infrastructure in managing their security risks?	Clear and regular communication around expectations with updates in light of the shifting threat landscape.
22	Do you think there are other preparatory activities that would assist in proactively identifying and remediating cyber vulnerabilities?	Yes, a cybersecurity self-assessment for identifying current practices and a gap analysis across all industries.
23	What information would you like to see shared with industry by Government? What benefits would you expect from greater sharing?	Government sharing of emerging risks, or issues arising for security threats (i.e. ASIO observations on cybersecurity incidents or emerging insider threats); and updates on companies that may be high risk (particularly sovereign risk) e.g. the case with Huawei.

		The sharing of registration information that has been provided by entities to the government.
25	What methods should be involved to identify vulnerabilities at the perimeter of critical networks?	This should follow existing ISO standards for cybersecurity testing (or equivalent) to ensure consistent testing.
26	What are the barriers to owners and operators acting on information alerts from Government?	For cybersecurity it is the timely communication and information sharing regarding attacks. There may be complexity in contracts with international service providers.
27	What information would you like to see included in playbooks? Are there any barriers to co-developing playbooks with Government?	Further detail is required on the PSO before this can be answered.
29	In what extreme situations should Government be able to take direct action in the national interest? What actions should be permissible?	This will differ depending on the industry but there needs to be strict safeguards and due process considered and implemented.
30	Who do you think should have the power to declare such an emergency? In making this declaration, who should they receive advice from first?	AGL would suggest the use of designated legislation/instruments to allow the high-level principles to be enacted in legislation but these integral questions to be discussed and debated through industry specific workshops and consultations. The exercise of this kind of power should be industry specific.
32	If, in an exceptional circumstance, Government needs to disrupt the perpetrator to stop a cyber-attack, do you think there should be different actions for attackers depending on their location?	This would depend on the nation state, Australia's relationship with them and expectations around co-operation
33	What sort of legal protections should officers (both industry and Government) undertaking emergency actions be afforded?	There should be some level of immunity for actions that have unintended adverse consequences, but the process requires more detail before those levels can be determined.
35	What are the risks to industry? What are the costs and how can we overcome them? Are there sovereign risks to investment that we should be aware of?	It is too early in the consultation process to determine costs as the detail required to do such analysis is lacking.