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.