16 September 2020

Department of Home Affairs
ci.reforms@homeaffairs.gov.au

Dear Sirs,

Essential Energy's Response to consultation paper on Protecting Critical Infrastructure and Systems of National Significance

Essential Energy welcomes the opportunity to respond to the Department of Home Affairs (the Government's) consultation paper on *Protecting Critical Infrastructure and Systems of National Significance*.

Essential Energy distributes electricity to almost 870,000 customers across 95 per cent of New South Wales (NSW) and parts of southern Queensland. We are owned by the NSW Government and employ approximately 3,000 people, mainly in regional NSW.

Essential Energy is already subject to a number of critical infrastructure obligations through conditions that were added to our IPART-administered Distributor's Licence in 2019. Any additional obligations arising out of the enhanced framework should be added to the existing regulatory arrangements. Essential Energy also recommends that the number of regulatory entities overseeing critical infrastructure compliance is not increased.

However, it is important these enhanced obligations are determined and applied using a risk-based approach. Essential Energy strongly recommends that the implementation of targeted arrangements that are commensurate with the risks being avoided is critical to avoid the imposition of unnecessary and inefficient costs on consumers.

The costs of complying with any new obligations will depend on the exact nature of the obligations and the work that Essential Energy needs to do to comply with those obligations. Any additional costs will need to be funded by customers and may result in higher electricity distribution prices for customers connected to the Essential Energy network.

Essential Energy would welcome the increased sharing of relevant information with the Commonwealth Government and other critical infrastructure entities, through the Trusted Information Sharing Network (TISN) or other reliable and secure means. The use of relevant playbooks that help critical infrastructure entities prepare for and mitigate specific threats would also be of value.

Essential Energy's detailed responses to the questions raised in the consultation paper are provided in **Attachment 1.**

Essential Energy looks forward to continuing to engage with the Commonwealth Government as it develops the frameworks and progresses towards implementation. If you have any questions in relation to this submission, please contact Natalie Lindsay, Head of Regulatory Affairs at [redacted] or via phone [redacted].

Yours sincerely

[redacted]

Chantelle Bramley
General Manager, Strategy, Regulation & Corporate Affairs

Attachment 1 – Response to Protecting Critical infrastructure Consultation Paper

Ref	Question	Essential Energy Response
Who will the enhanced framework apply to?		
1	Do the sectors above capture the functions that are vital to Australia's economy, security and sovereignty? Are there any other sectors that you think should be considered as part of these reforms (e.g. manufacturing)?	The Consultation Paper captures the key sectors that should be covered by the proposed reforms. In applying the reforms to sectors and sub-sectors it is important that a risk-based approach is applied which ensures that obligations applied to critical infrastructure entities are commensurate with the risks being avoided.
2	Do you think the current definition of Critical Infrastructure is still fit for purpose?	Essential Energy is currently required to comply with critical infrastructure obligations which are enacted through the *Ministerially imposed licence conditions for the operator of a distribution system* (the Licence). This Licence includes a definition which differs slightly to the Australian Governments critical infrastructure definition. Essential Energy suggest the definition be aligned as follows: *'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* ***security****, social or economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security.'* The definition as it applies to Essential Energy is very broad and captures many aspects of its operations. It is important that the underpinning regulatory framework to be implemented is targeted at, and commensurate with, the risks being avoided. Otherwise: • digitally based services for customers may be limited or prohibited; and • unnecessary and inefficient costs may be passed onto consumers through higher energy prices.
3	Are there factors in addition to interdependency with other functions and consequence of compromise that should be considered when identifying and prioritising critical entities and entity classes?	From an energy perspective, consideration of the supply chain in assessing interdependency with other functions is important. Some elements of the supply chain will present far higher risks due to their interconnectivity with other critical infrastructure and the location of that infrastructure. For example, a transmission network servicing an entire state presents more risk than a highly dispersed and segmented rural distribution network. Again, it is critical that a risk-based, proportionate approach is applied to each sector and sub-sector.
4	What are the common threats you routinely prepare for and those you have faced/experienced as a business?	Essential Energy currently prepares for, and face, a number of threats which have the potential to impact operations. These threats include: • distributed denial-of-service (DDoS); and • Malware Phishing and Ransomware.

Ref	Question	Essential Energy Response
		We have recently experienced a known malicious malware variant which impacted our internal infrastructure.
5	How should criticality be assessed to ensure the most important entities are covered by the framework?	Refer to Question 3
6	Which entities would you expect to be owners and operators of systems of national significance?	Refer to Question 3
Government-Critical Infrastructure collaboration to support uplift		
7	How do you think a revised TISN and Critical Infrastructure Resilience Strategy would support the reforms proposed in this Consultation Paper?	The Trusted Information Sharing Network (TISN) for critical infrastructure resilience has a very important role to share information with critical infrastructure entities. This will enable entities to proactively implement controls which will limit or eliminate the impact of potential threats.
8	What might this new TISN model look like, and what entities should be included?	Additional involvement from, or coordination with, operational agencies within state-based emergency management arrangements would be beneficial.
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?	There is an opportunity for additional cross-industry all hazards scenario planning to supplement exercises that focus on particular sectors or hazards, for example, GridEx.
10	Are the principles-based outcomes sufficiently broad to consider all aspects of security risk across sectors you are familiar with?	Essential Energy welcomes the principles-based outcomes outlined in the consultation paper. Identifying and understanding risks, including an assessment of consequence should ensure that any controls identified and implemented are commensurate with the identified risk. However, Essential Energy cautions against creating an overly burdensome regulatory framework which focuses too much on administrative approaches to risk management, policies and procedures rather than outcomes.
11	Do you think the security obligations strike the best balance between providing clear expectations and the ability to customise for sectoral needs?	Yes. Clear obligations are necessary to ensure: • the implementation of appropriate measures is matched against the risk and consequences of harm; • unambiguous direction is provided to critical infrastructure entities; and • sufficient funding for efficient compliance activities is approved through regulatory determinations.
12	Are organisations you are familiar with already operating in-line with these principles, or do you think there would be a	As discussed in Question 2, Essential Energy is already subject to critical infrastructure obligations through the Licence which is regulated by the Independent Pricing and Regulatory Tribunal

Ref	Question	Essential Energy Response
	significant time and/or financial cost to meet these principles?	(IPART). The cost and time to implement these obligations is significant. Any additional security obligations need to: • be applied using a risk-based approach • avoid duplication of existing requirements; • be cognisant of the fact that consumers will be required to fund the implementation of any additional obligations.
13	What costs would organisations take on to meet these new obligations?	Incremental costs would be dependent upon the exact nature of any new security obligations. Improving an organisation's cyber security maturity can be very expensive, as can improvements to physical, supply chain and personnel security arrangements. Thus, careful consideration of a risk-based approach in applying these new obligations is crucial. As discussed above, Essential Energy is already subject to critical infrastructure obligations which are significant and will be costly to fully implement.
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?	Refer to Question 13
Regulators		
15	Would the proposed regulatory model avoid duplication with existing oversight requirements?	If the intent is to expand and enhance existing regulatory frameworks, Essential Energy suggests that any new obligations for NSW are included within the Distributor's Licence. This would avoid duplication in regulatory arrangements and limits the number of regulatory entities which are involved.
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?	Within the distribution sector there are a number for regulators which either focus on economic and consumer protection issues, or safety and technical matters. Critical infrastructure and cyber security matters are not often in the expertise areas of existing regulators. A broad range of communication and engagement strategies is required, this could take the form of security briefings to the most senior members of an organisation through to industry working groups to allow for collaboration on common issues. Regulator guidance on how to interpret and meet obligations is also important, particularly when new obligations are being implemented. This guidance could be in the form of plain English guidelines that explain the expectations of what is and is not acceptable from a compliance perspective. This should be made available to those entities which are required to meet the obligations.

Ref	Question	Essential Energy Response
		Regulatory approval of an implementation plan that itemises the steps required to comply with the new obligations can also be a tool to provide guidance.
17	Who would you consider is best placed to undertake the regulatory role for sectors you are familiar with? Does the regulator already have a security-related regulatory role? What might be the limitations to that organisation taking on the role?	As discussed above, within NSW, IPART already regulates compliance with critical infrastructure obligations and they would be best placed to enforce compliance with any additional obligations.
18	What kind of support would be beneficial for sector regulators to understand their additional responsibilities as regulators?	Essential Energy's preference is to build on and enhance existing regulatory frameworks and that oversight of current regulatory bodies is maintained. However, as discussed in Question 16, critical infrastructure and cyber security matters are not often in the expertise areas of existing regulators. Australian Government support is required for regulatory bodies which are required to enforce critical infrastructure obligations. This support should be in the form of education, engagement and regulator forums to ensure the translation of Australian Government objectives into regulatory arrangements is consistent and proportionate.
19	How can Government better support critical infrastructure entities in managing their security risks?	Government can better support critical infrastructure entities by: • adopting a risk-based approach to standards and requirements, • providing a clear delineation and separation between privacy and security risks in relation to data; and • more practical guidance on exemptions and situations in which offshore access and/or storage of information may support the objectives of the legislation (e.g. redundancy and access to specialist offshore vendor support).
20	In the AusCheck scheme, potential and ongoing employees in the aviation, maritime, health and major national event security sectors undergo regular national security assessments by the Australian Security Intelligence Organisation and criminal history assessments to mitigate the risk of insider threats. How could this scheme or a similar model be useful in the sectors you are familiar with?	A small number of critical roles may benefit from additional background checks and information sharing similar to the sectors in the AusCheck scheme.
21	Do you have any other comments you would like to make regarding the PSO?	As discussed above the Positive Security Obligation (PSO) should: • avoid duplication of existing regulatory frameworks • not increase the number of regulatory entities; overseeing critical infrastructure compliance;

Ref	Question	Essential Energy Response
		• implement targeted arrangements that are commensurate with the risks being avoided, and • avoid the imposition of unnecessary and inefficient costs on consumers.
Enhanced Cyber Security Obligations		
22	Do you think there are other preparatory activities that would assist in proactively identifying and remediating cyber vulnerabilities?	Direct integration with internal threat and vulnerability management systems to a Commonwealth system would assist with detection/reporting vulnerabilities. This together with a sector wide analysis of the external presence of critical infrastructure providers (remote access, web etc.) would enable organisations to reduce the amount of effort required to manage the most obvious ingress paths.
23	What information would you like to see shared with critical infrastructure by Government? What benefits would you expect from greater sharing?	Shared threat intelligence would benefit the sector. The ability to respond during the event of an incident as a sector would greatly improve with a shared platform to both receive and share threat intelligence.
24	What could you currently contribute to a threat picture? Would you be willing to provide that information on a voluntary basis? What would the cost implications be?	Essential Energy has invested heavily in advanced detective and investigative capabilities that allow timely reporting and analysis of threats to many of our systems. Whilst our capability is still relatively immature, the technologies upon which our capabilities are built are known to provide accurate information which may indicate trends when coupled with other sources of threat intelligence, to provide actionable sector specific intelligence. Although provision of such information would be voluntary, it would require appropriate handling whilst in an attributable form.
25	What methods should be involved to identify vulnerabilities at the perimeter of critical networks?	Maturity assessments have limited benefit as a means of identifying vulnerabilities. Given any policy, process or outcomes of cyber capability uplift, it should remain necessary that controls are technically verified. Technical verification of controls will then support identification of what vulnerabilities remain and what mitigative controls remain on hand to be applied.
26	What are the barriers to owners and operators acting on information alerts from Government?	Our current cyber security maturity level, specifically as it relates to processes and procedures, ensures that alerts are actioned effectively and in a timely manner. However, Essential Energy's Licence requires that some senior officers within Essential Energy must hold an appropriate national security clearance (bearing a clearance of not less than Negative Vetting Level 1). Despite Essential Energy's compliance with these obligations, it is unclear how the employees that hold national security clearance have ongoing access to information or appropriate communication channels.

Ref	Question	Essential Energy Response
		Essential Energy expects that these employees should have access to important information alerts to ensure that potential threats can be effectively dealt with.
27	What information would you like to see included in playbooks? Are there any barriers to co-developing playbooks with Government?	Playbooks that relate specifically to identified threats which may force the involvement of government agencies such as the CIC, ASD/ACSC or ASIO would be useful i.e. a playbook that can be used in a break glass emergency once the threat meets the most critical criteria. In terms of barriers, provided there is a demarcation between a standard operational playbook versus a playbook that involves the Commonwealth then this should allow a tangible outcome as per above. Limiting the scope will be key.
28	What safeguards or assurances would you expect to see for information provided to Government?	Appropriate support (if infrastructure is needed) and security controls, such as encryption.
Cyber assistance for entities		
29	In what extreme situations should Government be able to take direct action in the national interest? What actions should be permissible?	When an immediate and significant threat is detected, Government should communicate and work with critical infrastructure entities to effectively avoid, mitigate or reduce the threat.
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?	n/a
31	Who should oversee the Government's use of these powers?	n/a
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?	No, the action and activity required to disrupt and stop an attack should be consistently applied, regardless of the location of the attackers. The priority is the containment, eradication and restoration of the key business process.
33	What sort of legal protections should officers (both industry and Government) undertaking emergency actions be afforded?	n/a
34	What safeguards and oversight measures would you expect to ensure the necessary level of accountability for these type of powers?	n/a
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?	Risk of disruption to services is fundamental to critical infrastructure operators. The addition of a regulatory layer to formalise how these risks are managed is appropriate, however, a proportionate approach to costs and benefits should be applied at a more granular level, e.g. there is a risk that

Ref	Question	Essential Energy Response
		unnecessary time, cost and resources are dedicated to mitigation of low-consequence risks which pose minimal risk to continuity of services or resilience of critical infrastructure.
36	Does this mix of obligations and assistance reflect the roles and responsibilities of Government and industry in protecting critical infrastructure? How would private sector management of risk change with the proposed increased role for Government?	Management of risks to reliability, security and privacy are becoming more linked and complex. With an increased role of Government, there should also be increased responsibility and coordination of overlapping and inconsistent regulations from different regulators, instruments and conditions for managing these risks.