Consultation Paper Response

Protecting Critical Infrastructure and Systems of National Significance

Submission from Endeavour Energy

Endeavour Energy

Questions to respond

2) Do you think the current definition of Critical Infrastructure is still fit for purpose?

- The industry has multiple interpretations of the same Critical Infrastructure regulations and has different usage of terminologies for type of data. Due to this difference in understanding and interpretation, critical infrastructure assets or associated technology assets are protected inconsistently across the industry.
- There needs to be clarity around the scope of the critical infrastructure assets, associated technology assets and the sensitives data types. There is an imperative need to standardise the definition of critical infrastructure, associated technology assets and data types. A consistent definition helps in applying appropriate security and avoids miscommunication and risk exposures.
- It is essential to ensure that these definitions align with International Standards or Australian Standards such as AS/NZS/ISO/IEC.

10) Are the principles-based outcomes sufficiently broad to consider all aspects of security risk across sectors you are familiar with?

Energy Industry uses several International Standards or Australian Standards such as

- Asset Management is ISO 55001;
- Health and Environmental Safety ISO 14001;
- Risk Management ISO 31000; or
- Information Security ISO 27001, ISO 27002 and ISO 27019,

It is essential to ensure that security standards align to already existing International or Australian Standards to ensure easy adoption and alignment with existing practices.

13) What costs would organisations take on to meet these new obligations?

- It is critical to understand the details of the new obligation around Physical Security, Cyber Security, Personnel Security and Supply Chain Security. This will help us put a plan in place and estimate the cost of compliance.
- It is important to note that obligations must be based on organisations business risks and potential security exposures. Risk-based approaches to security provide justification for specific security investments. This allows the organisations like Endeavour Energy to tie the investments directly to the hazards that they mitigate and the value that this brings to the organisation.

15) Would the proposed regulatory model avoid duplication with existing oversight requirements?

The Regulatory Model demonstrates a reasonably practical operating model between Australian Energy Market Operator (AEMO), Australian Cyber Security Centre (ACSC), Critical Infrastructure Centre (CIC) and the Cyber Security Industry Working Group (CSIWG); therefore, duplication must be avoided. At present, the Commonwealth sets the outcomes with IPART or AEMO, who work with industry to monitor and enforce specific standards for compliance obligations. It is essential to ensure all regulatory stakeholders are identified; their requirements are incorporated and communicated to ensure consistency in compliance.

21) Do you have any other comments you would like to make regarding the PSO?

The top three support comments to summarise the effective implementation of Positive Security Obligation are;

- There must be clarity in scope, the definition of data, security standards and timeframes provided to achieve Positive Security Obligation;
- The implementation of control MUST be based on risk exposure; and
- Positive Security Obligation should be based on industry-accepted international standards. Positive Security Obligation must reduce duplicate obligations from Industry Regulators, State Government and Commonwealth Govt.