AEMO
AUSTRALIAN ENERGY MARKET OPERATOR

Level 22
530 Collins Street
Melbourne VIC 3000

Postal address
GPO Box 2008
Melbourne VIC 3001

T 1300 858 724
F 03 9609 8010
E info@aemo.com.au

12 April 2023
Expert Advisory Board
Department of Home Affairs and Cyber Security
PO Box 25,
Belconnen ACT 2616

Online submission

Dear Expert Advisory Board,

2023-2030 Australian Cyber Security Strategy

AEMO supports the development of a 2023-30 cyber security strategy (the Strategy) and welcomes the opportunity to respond to the recently released discussion paper. There is a clear and pressing need to review Australia's cyber security strategy, as technology and digitalisation continues to transform the Australian and global economy, allowing critical products and services to be increasingly delivered through new and decentralised business models.

AEMO, as the energy system and market operator[1] is at the forefront of energy transformation which is expected to accelerate out to 2030. Our role is to ensure safe, reliable and affordable energy today and enable the energy transition to net zero for the benefit of all Australians. This presents many opportunities and risks, with cyber security being critical with respect to the latter. As the cyber security strategy could support the security and reliability of electricity and gas systems, AEMO is highly engaged in and seeking to contribute to its development.

The approach set out in the discussion paper including the core and potential policy areas is logical and sound. The establishment of an expert advisory board and a focus on fostering partnerships across Governments, industry, academia and regions are positive developments that provide scope to leverage a range of skills and experience. As acknowledged in the discussion paper, the Strategy can draw from and complement recent and current reforms, namely the *Security of Critical Infrastructure Act 2018* (SOCI Act) as well as the current Privacy Act review triggered by significant customer data breaches in late 2022. The core policy area of enhancing and harmonising regulatory frameworks identified in this discussion paper was also a key tenet of the recent SOCI Act reforms.

AEMO supports the enhancement and harmonisation of regulatory frameworks for cyber security as this can drive improved cyber security resilience, facilitate greater visibility and a better understanding of cyber security requirements and reduce compliance costs. As such, AEMO considers that there may be merit in investigating

[1] AEMO operates the bulk power system and wholesale electricity market in the eastern and south-eastern Australia, the National Electricity Market (NEM) as well as Western Australia's South-West Interconnected System power grid and its associated Wholesale Electricity Market. AEMO manages a number of wholesale gas markets including the Short Term Trading Markets in Brisbane, Sydney and Adelaide and the Gas Supply Hubs in Wallumbilla in Queensland and Moomba in South Australia. In Victoria AEMO operates the Victorian Gas Declared Transmission System and manages the Victorian Declared Wholesale Gas Market.

the creation of a Cyber Security Act, providing a holistic approach to cyber security considerations, requirements and obligations.

Cyber security regulatory frameworks need to account for interdependencies between key sectors, which has been and will continue to be driven by technological advancement and digitalisation. For instance, the electricity sector is highly reliant on telecommunications services in managing both energy systems and markets, while the transport sector will be increasingly reliant on the electricity sector with the uptake of electric vehicles. Further, end-use consumer uptake of digitally connected devices that are expected to play a critical role in energy security and reliability, introduce additional cyber security risks into the supply chain. The risk of contagion from a cyber security event within a sector and across sectors needs to be continually assessed given its evolving nature. It is important the cyber security regulatory frameworks account for sector dependencies as well as have the scope to define sector-specific requirements.

AEMO is aware that cyber security requirements will need to change in the energy sector as the transition gathers pace. Key features of the transition include a system consisting of an increasingly decentralised generation and storage asset base and the provision of services by an increasing number of market participants including empowered customers. While there is a concerted effort in the energy industry to define the new technical requirements for the energy system of the future, considerable uplift is required in this area to ensure that system security and reliability can continue to be delivered, including a focus on and consideration of cyber security requirements.

Understandably the Strategy and any ensuing regulatory reform may have a strong focus on the protection of and access to customer data, given recent data breaches. While this is entirely appropriate, AEMO would recommend that the Strategy and regulatory reform provides an equal focus on cyber security and resilience for industrial control systems and “internet of things”. In addition, the Strategy and regulatory reform should be as forward-looking as possible. Artificial Intelligence (AI) is expected to be widely prevalent by 2030 and potentially instrumental in the control of critical assets and delivery of critical services. The opportunities offered by AI are significant, as are the risks including around cyber security. Regulatory reform often lags changes to business models or new products and services. Ensuring that regulatory frameworks keep pace with fundamental changes such as AI is essential, otherwise risks will not be adequately managed.

Moreover with regards to compliance, AEMO would recommend a strong compliance regime be incorporated into any cyber security regulatory framework, as the potential costs of material cyber security events are substantial. This will rely on the effective definition of roles and responsibilities. It is important to note that the investment requirements to deliver on the vision of be the world’s most cyber secure country by 2030 will be very significant and appropriate avenues to fund upgrades across critical infrastructure and systems will need to be identified.

AEMO recognises the importance of having a comprehensive and forward-looking cyber security strategy and regulatory framework that protects and supports the Australian economy and way of life. Many other Governments are similarly developing national cyber security strategies including the United States[2] and AEMO would encourage the Expert Advisory Board to draw from international approaches and insights where appropriate.

[2] FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy | The White House

We look forward to contributing to the policy debate and regulatory reform processes. Should you wish to discuss this submission or opportunities for AEMO to further contribute, please contact Kevin Ly, General Manager of Reform Developments & Insights on [redacted] or [redacted].

Yours sincerely,

[redacted]

Violette Mouchaileh

Executive General Manager – Reform Delivery