Level 22
530 Collins Street
Melbourne VIC 3000

Postal Address:
GPO Box 2008
Melbourne VIC 3001

T 1300 858724
F 03 9609 8080

16 September 2020

Michael Pezzullo
Secretary
Department of Home Affairs
PO Box 25,
BELCONNEN, ACT 2616

By online submission: ci.reforms@homeaffairs.gov.au

Dear Mr Pezzullo

Protecting Critical Infrastructure and Systems of National Significance Consultation – AEMO Submission

AEMO is pleased to make this submission on the Protecting Critical Infrastructure and Systems of National Significance (SoNS) Consultation Paper (the Consultation Paper).

The recent publication of the Commonwealth Government's Cyber Security Strategy 2020 and these reforms are both critical steps in safeguarding the provision of essential services, including energy services, that underpin our economy, security and sovereignty.

AEMO supports the proposed approach of making enhancements to the existing framework in the *Security of Critical Infrastructure Act 2018 (Cth)* (the Act), underpinned by collaborative activities between Government and industry that will improve our collective understanding of risk across sectors, and uplift the security and resilience of critical infrastructure. There is a clear and demonstrated need to establish national, principles-based and proportionate requirements, that secure the provision of essential services on a collaborative, sustainable and affordable basis.

AEMO has been progressing its cyber security and resilience capabilities and maturities since 2018, in response to the Finkel Review recommendations. The focus of this work has been both internal, resulting in a significant cyber uplift across AEMO's systems, personnel and supply chain, as well as facilitating cyber maturity across the energy sector. In collaboration with the Australian Cyber Security Centre (ACSC), the Critical Infrastructure Centre (CIC), and industry, AEMO has been instrumental in the establishment and implementation of Australian Energy Sector Cyber Security Framework (AESCSF). This has included the promotion of greater industry information exchanges and the delivery of industry training and exercise regimes, and has prepared AEMO and many electricity industry participants well for the forthcoming regulatory framework changes. AEMO is supportive of the Government's intention to leverage and enhance existing voluntary arrangements, such as the AESCSF, to support the enhanced regulatory framework.

The role of Government is critical to driving effective cross-sector collaboration and preparedness, and AEMO is supportive of this as a key feature of the reforms. AEMO has been working closely with the Department of Industry, Science, Energy and Resources (DISER), and through the Cyber Security Industry Working Group (CSIWG), to support development of a Roadmap for Improving Cyber Security in the Energy Sector (the Roadmap). As agreed at the (former) COAG Energy Council meeting in March 2020, AEMO will continue to develop the AESCSF, including reviewing and extending the framework to the gas sector and reporting annually on cyber security preparedness, which will form a key component of the Roadmap in the energy sector.

Given the close and collaborative working relationship between the Australian Government, the market bodies and industry, AEMO's submission is high-level and brief, focussed on five key issues (see Attachment A) for consideration by the Department of Home Affairs through the next stage of development of the enhanced framework and co-design of sector specific standards and requirements.

AEMO agrees that protecting critical infrastructure and SoNS is a priority for Government, the market bodies and industry, and would welcome early and ongoing consultation on legislative and sector specific requirements and criteria. Effective partnership between Government and critical infrastructure industries is paramount to achieving security objectives, and AEMO looks forward to working closely with the Department of Home Affairs as the reforms and legislative design progress.

For further information on the AEMO submission, please do not hesitate to contact myself or Tim Daly, Chief Security Officer on [redacted].

Yours sincerely

[redacted]

Tony Chappel
Chief External Affairs

Attachment A

ATTACHMENT A: PROTECTING CRITICAL INFRASTRUCTURE AND SYSTEMS OF NATIONAL SIGNIFICANCE - AEMO SUBMISSION

1 An integrated cyber security framework for the energy sector

In delivering our inaugural 2018 Summary Report into the Cyber Security Preparedness in response to the Finkel Review recommendations, AEMO concluded that current provisions in the National Energy Laws and Rules frameworks are inadequate to address cyber security risk. Specifically, AEMO recommended changes to the National Electricity Law (NEL) to ensure that AEMO has a clear statutory function to address cyber security risks in the National Electricity Market (NEM). Any changes should also apply to the Western Australian Wholesale Electricity Market (WEM) and to gas under the National Gas Law (NGL).

To achieve an effective cyber security regime for the energy sector, amendments to the Cth Act need to take account of existing statutory and regulatory frameworks in the energy sector. Unlike many other sectors to which the Act is intended to apply, the legal framework for the energy sector is governed by a national co-operative legislative regime which applies a set of "national" but State / Territory-based laws and rules to each of the participating jurisdictions[1].

In addition, each State and Territory has specific local requirements that potentially overlap with cyber security requirements. These include licensing regimes which mandate local standards that operate concurrently with the national energy market arrangements.

The changes to the Cth Act and other cyber regulatory implementation initiatives will be most effective if existing frameworks at Commonwealth and State/ Territory levels can operate alongside of the enhanced security and cyber framework. If energy-specific changes are needed, these should be integrated in an orderly way into the existing frameworks, which may include changes to the applicable laws and rules.

2 Clarity on roles and responsibilities and limiting duplication

Emergency arrangements for safety and security of the energy sector are well established and understood. AEMO's electricity emergency arrangements provide a framework for the coordination of electricity emergencies across the NEM, setting out the roles and responsibilities of AEMO, government, and industry. The NEM jurisdictions and AEMO have a Memorandum of Understanding and an Emergency Protocol to co-ordinate actions to be taken under individual State / Territory legislation to manage power system security emergencies (for example in section 117 of the NEL).

[1] The legal framework in the non-NEM States and Territories is fragmented. The WEM operates under separate legislation, the Western Australian Electricity Industry Act 2004 and the Electricity Industry (Wholesale Electricity Market) Regulations 2004. A modified version of the NGL operates in Western Australia under the National Gas Access (WA) Act 2009. A modified version of the NEL operates in the Northern Territory under the National Electricity (Northern Territory) (National Uniform Legislation) Act 2015.

The proposed critical infrastructure and SoNS regulatory framework includes Government having a role in assisting entities in response to significant cyber-attacks on Australian systems. A response model is put forward with proposed responsibilities, including situations where the Government may issue a direction or declare an emergency (resulting in their taking direct action). AEMO agrees there are benefits in establishing Government assistance arrangements for all critical infrastructure and SoNS in response to cyber-attacks. Greater clarity on roles and responsibilities under the proposed Government assistance arrangements is needed however, including consideration of how these arrangements would operate effectively alongside existing emergency arrangements.

The design of sector specific requirements for Positive Security Obligations areas should be specific, measurable, attainable, realistic and timely. AEMO recommends that this be informed by, and leverage the AESCSF, which has been adopted by much of the industry. The AESCSF covers a range of domains including three of the four Positive Security Obligation areas – cyber, personnel and supply chain. Extending the AESCSF domains to incorporate physical security should be considered and advanced. AEMO would value some further clarity about how the standards will be enforced through the sector-specific consultation processes.

3 Funding implications of additional responsibilities under the enhanced framework

AEMO, along with other owners and operators of critical infrastructure and SoNS, will be required to the meet to the costs of security uplift and ongoing compliance with the enhanced framework. The nature and scope of the enhanced obligations and roles under the Cth Act, and the development and implementation of the energy specific standards, will have additional resourcing and funding implications for AEMO.

In addition, AEMO's work with DISER and CSIWG on the Roadmap for Improving Cyber Security in the Energy Sector, contemplates a number of new or expanded lead and support roles for AEMO, including for example, expanding the AESCSF to gas and non-NEM / WEM jurisdictions; reviewing the AESCSF; developing and running sector wide exercises to test preparedness; formalising arrangements for debriefing after incidents; and developing guidance on "responsible cyber security practice".

Further consideration of how these increasing levels of responsibility and activity will be resourced and funded, including within the context of AEMO's fee structure, is needed. AEMO is a not-for-profit company limited by guarantee, with government and industry members. AEMO receives no ongoing government funding, and recovers its operating and capital expenses through approximately 20 different fees levied on participants. Each fee is limited to the costs of providing that particular service, and AEMO's annual budget is consulted on each year. AEMO's current fee structures for the NEM and under the NGR expires on 30 June 2021. As required by the National Electricity and Gas rules, AEMO has initiated a separate consultation to discuss optimum fee structures for July 2021 commencement.

As highlighted above, AEMO has previously recommended changes to the NEL to provide AEMO with a clear statutory function to address cyber security risks in the NEM. This should also be extended to the WEM and the NGL, particularly given the COAG EC's request to extend the AESCSF to the gas sector. This is important, and requires further consideration and discussion with the Department as the framework is developed, to ensure that AEMO is able to justifiably recover the costs from participants associated with security compliance obligations, continuing to enhance our own security capability as market and system operator, and supporting ongoing energy sector cyber security maturity through the AESCSF and the Roadmap under the existing State / Territory frameworks.

4 Critical Infrastructure and Cyber Regulators

Given the potentially significant impact of a cyber security breach for the energy sector, and the risk of negative implications for critical infrastructure, the economy and communities, AEMO has firmly been of the view that a voluntary, self-regulated approach is not an adequate or sustainable arrangement. AEMO is therefore pleased that the consultation paper recognises the need for improved regulation of critical infrastructure and cyber security as part of the enhanced framework.

The consultation paper recognises that a one-size-fits-all approach to regulation is not appropriate given the range of sectors to which the framework will apply, and that there are various standards and requirements already in place for some sectors. As such, the Department will work with critical infrastructure entities to identify the most appropriate regulator for each sector. The proposed framework identifies designated sector Regulators to work with entities to co-design, monitor and enforce sector-specific standards across physical, cyber, personnel and supply chain security to underpin the Positive Security Obligation.

The consultation paper also proposes enhanced cyber security obligations for owners and operators of SoNS aimed at strengthening the resilience of these systems, to be regulated by the Department of Home Affairs.

As previously advised, it is not appropriate for AEMO to assume the role of a regulator to monitor and enforce compliance, as AEMO is itself subject to the security regime, a number of industry participants are AEMO members, and AEMO has other roles that are not compatible with regulator functions.

AEMO is therefore supportive of a Commonwealth-led regulator model tailored to the energy sector, drawing on lessons and experience gained from other critical infrastructure sectors. Ideally, a single, holistic and consistent regulator responsible for monitoring, enforcement and reporting of both the sector-specific standards and the enhanced cyber security requirements, would be most effective and efficient. In addition, to the extent possible, cyber security monitoring, reporting and information sharing should leverage, or build upon, the approach that is undertaken through the AESCSF. AEMO could play a technical advisory / support role if this would assist the regulator in the performance of its function. This would, however, have additional resourcing and funding implications for AEMO (see discussion above).

5 Coverage of the Enhanced Regulatory Framework

The consultation paper explores which entities will be covered by the enhanced framework, including the different classes of entities (critical infrastructure assets, regulated critical infrastructure assets and SoNS), and the elements of the framework that will apply to each. A mapping process will be conducted using criteria to be developed on a sector specific basis, taking account of an entity's internal characteristics and the external operating environment, focused at the owner and operator level, not at a specific piece of technology.

For the energy sector, the application of the enhanced regulatory framework requires further consideration and consultation. There is scope to leverage the AESCSF's criticality assessment tool (CAT), in terms of defining sector-specific criteria. AEMO considers CAT to be a good starting point, noting that improvement opportunities have been identified as our understanding of sector vulnerabilities and criticalities continually progresses.

As the market and system operator, AEMO considers the criteria for classifying entities, should take account of the following factors:

- entities' interaction with AEMO's key market systems (for example Market Settlements and Transfer Solutions, Energy Management System, Energy Market Management System);
- the role of entities in providing ancillary support services to AEMO and transmission network service providers;
- The interdependencies and risks associated with existing market participants (e.g. major industrial loads of 100MW and greater); and
- The potential interdependencies and risks of new and emerging technologies and participants in the energy sector, such as distributed energy resources (DER), virtual power plants (VPPs), and demand response service providers.

AEMO is currently consulting on an initial DER minimum technical standard to enable the required capability to underpin power system security and reliability. Minimum technical standards will set out cybersecurity requirements, although these will not to be incorporated into this initial DER standard as further industry consultation to develop to a point capable of being implemented is required. Given the transformational changes and the reform agenda taking place, it is important that the enhanced regulatory framework as applies to the energy sector can readily accommodate change and be dynamic over time.