01/11/2019

Level 22
530 Collins Street
Melbourne VIC 3000

Postal Address:
GPO Box 2008
Melbourne VIC 3001

T 1300 858724
F 03 9609 8080

Hon Peter Dutton
Minister for Home Affairs
PO Box 6022
Parliament House
Canberra ACT 2600

By online submission

Dear Mr Dutton

Australia's 2020 – Cyber Security Strategy

Thank you for the opportunity to provide a submission to Australia's 2020 Cyber Security Strategy.

AEMO shares the Government's view that cyber security and the safety of our internet is important to protect our essential services, such as energy, water and transport. The pervasive use of information and communications technology and its convergence with operational technology renders critical systems and infrastructure vulnerable to cyber-attack. The rapid transformation of the energy sector extends to cyber security.

The Government's request for submissions into the development of Australia's next Cyber Security Strategy, is an important step toward an economy-wide policy and regulatory approach to cyber security of our essential services going forward. This is because the existing cyber security regulation in Australia is fragmented, without specific regulatory oversight or centralised regulatory regime in Australia.

To ensure cyber safety across all sectors of our economy, AEMO supports a broad workstream, led by Government in collaboration with industry to establish a comprehensive regulatory framework. Such a framework should establish cross-sectoral standards and ensure that these are not compromised amongst competing priorities.

To start to address these issues, AEMO is currently working with industry on a work program to improve cyber security preparedness in the energy sector. This led to the release of the Cyber Security Regulatory Reforms Report on 1 July 2019 with recommendations that underpin the development of a strong regulatory response to cyber risk in the interconnected energy system.

A further initiative, related to cyber security which is currently being dicussed with the Commonwealth, is the proposed Australian Energy Simulation Centre (AESC). A joint AEMO/CSIRO initiative, the AESC is a valuable tool that could allow detailed "what if" analysis of the consequences of malicious cyber activity in our rapidly digitising energy network and hence enhance the resilience of our critical energy infrastructure and associated communications and IT systems.

Our response to the Strategy Paper has been informed by the research and consultation that was undertaken as part of Cyber Security and Regulatory Reforms report. Given our commitment to addressing cyber security risks, and our current work with government and industry, we have not sought to address all the questions in the draft Cyber Security

Strategy, rather we have provided some targeted comments aimed at supporting the future direction of the Strategy and a nation-wide cyber security regulatory regime.

We would welcome the opportunity to discuss the matters raised in this submission further. Should you have any questions, please contact Kevin Ly, Group Manager Regulation on [redacted]

Yours sincerely

[redacted]

Tony Chappel
Chief External Affairs Officer

ATTACHMENTS: AEMO’s submission to Australia’s 2020 Cyber Security Strategy

KEY POINTS

- AEMO welcomes the development of Australia's next Cyber Security Strategy;
- AEMO supports the Government's approach to proactively addressing national, cross-sectoral cyber threats, which can be informed by work undertaken in the energy sector to date;
- Efforts in the energy sector should continue to be progressed while a comprehensive, national approach to cyber security is agreed;
- While industry is actively investing in the capabilities needed to manage cyber security risks, the role of Government is critical to driving effective cross-sector collaboration and preparedness
- AEMO notes the Government's priorities in this area and that resources should be deployed to the areas of greatest risk, including protection of critical infrastructure, and monitoring the potential cyber security risks of new products coming into the Australian market.

1. Introduction

AEMO welcomes the opportunity to respond to the Department of Home Affair's call for views on Australia' 2020 Cyber Security Strategy (the Strategy).

As the independent market operator for Australia's major electricity and gas systems, AEMO is focused on the secure, affordable and reliable supply of energy to Australian consumers and businesses. AEMO operates the market systems that facilitate wholesale and retail energy markets, working with generators, transmission and distribution companies to achieve this objective. AEMO agrees with the Government's view that cyber security is integral to these markets and the physical security of energy systems in an increasingly digitised business and operational environment.

Australia's energy sector faces escalating cyber threats from across the spectrum of hostile actors. The interconnected nature of our energy networks, energy's status as critical infrastructure, and the transformational changes occurring in the sector all increase the cyber vulnerability of our country. While industry is actively investing in the people, processes and technologies needed to manage cyber security risks, the risk cannot be remediated by industry alone. A strong partnership with Commonwealth and State Governments is critical to effectively manage the threat posed by sophisticated actors as well as the emergent cross-sectorial risks that come with the increasing sector convergence in our economy.

AEMO considers that voluntary industry activity and status quo regulatory arrangements cannot adequately address the growing level of cyber security risk and incidence, and therefore supports the Government's initiative to develop a nation-wide cyber security regulatory regime. The energy sector is now at a critical juncture and there is a pressing need to consider a common, cross-sectoral regulatory response to cyber security. Such a strategy can be informed by the work that AEMO has done to date.

Given our commitment to addressing cyber security risks, and our current work with government and industry, we have not sought to address all the questions in the draft Cyber Security Strategy; rather we have provided some targeted comments aimed at supporting the future direction of the Strategy and a nation-wide cyber security regulatory regime.

2. AEMO’s contribution to developing a cyber security strategy for the energy sector

In 2018, AEMO worked with industry and governments to develop a tailored cyber security framework for the Australian energy sector called the Australian Energy Sector Cyber Security Framework (AESCSF). This work culminated in a report to the Energy Security Board (ESB) on the Cyber Security Preparedness of the National and WA Wholesale Market in December 2018 (2018 Cyber Preparedness Report), responding to recommendation 2.10 of the Report into the Future Security of the National Electricity Market (Finkel Report).

The outcomes of this report show that cyber security strategies outside the regulatory frameworks, are limited in its reach. Investments in cyber security compete with commercial interests and it is challenging to convince Boards and economic regulators to commit funds without the regulatory need to do so.

The AESCSF self-assessments were undertaken by 270 market participants. Within the NEM, market participant response rates exceeded 60% in all sub-sectors with 100% of TNSPs and major DNSPs receiving facilitated self-assessments. Within the WEM, response rates were lower. Please refer to Figure 1 for an overview of coverage of market participants.

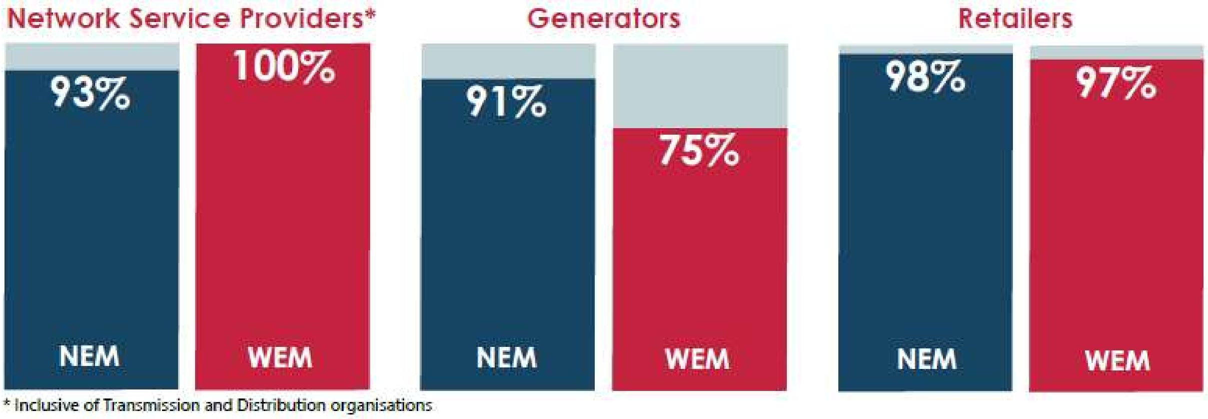

Figure 1 Coverage of market participants

The self-assessment identified opportunities to improve cyber security maturity across the sector. The cyber maturity responses considered how market participants raise cyber security awareness across their workforce to detect and report potential cyber security incidents.

The outcomes of this self-assessment test show that while industry is investing in cyber security capabilities, there are a range of challenges in problems with pursuing a voluntary, market-led program of work to address cyber security risks in the energy sector, pointing to the need for a nation-wide regulatory regime underpinned by tighter regulatory oversight across sectors. Examples of identified challenges or problems include:

- There is not a 100% coverage of support for the program, leaving organisations exposed to risks, that pose sectoral risks;
- Participants face conflicting priorities, balancing cyber security investment with cost/budget/revenue pressures and other priorities. While implementation of base level security capabilities is within the current plans of energy sector organisations, maturing these capabilities will require focussed and sustained investments in people, processes and technologies, and it can be challenging for organisations to establish the business case for these investments;

- The nature of cyber security threats means that businesses are subjected to risks if any of their sectoral counterparts fail in their efforts to effectively protect implement cyber security measures. In this sense, energy sector participants can be viewed as being exposed to the weakest link when it comes to cyber security.

Given the potentially significant impact of a cyber security breach for the energy sector, and the risk of negative implications for other critical infrastructure, the economy, national defence and Australian communities, AEMO is firmly of the view that a voluntary, self-regulated approach is not an adequate or sustainable response.

In addition to the self-assessment test, AEMO established the readiness and resilience working group to ensure that the sector has the processes and protocols in place to respond effectively to significant cyber incidents. This group which consists of representatives from across the Commonwealth, State and Territory Governments and the energy industry has defined the Australian Energy Industry Serious Cyber Incident Response Plan (AEISCIRP). This plan harmonizes Commonwealth, State and Territory, and industry efforts when responding to significant incidents affecting the energy sector and will be evaluated in GridEx V.

AEMO, in partnership with the CSIRO, is also in discussion with Commonwealth Departments, including the Department for Home Affairs, about potential funding for an Australian Energy Simular Centre,

At its heart, the AESC proposal is a “digital twin” of the live National Energy Market environment which would provide for numerous tools to help with planning and preventing malicious cyber activity targeting our critical energy infrastructure.

Also, In addition to our work in response to 2.10 of the Finkel recommendation AEMO prepared and submitted the Cyber Security Regulatory Reforms Report, released in July 2019 and subsequently provided to the Senior Committee of Officials (SCO) in August 2019.

This report considered the best-practice regulatory approaches to address cyber security problems in Australia’s interconnected energy systems.

The Report outlines options to implement reforms in the energy sector and formed a set of preliminary recommendations on an approach to protect Australia’s energy system from cyber threats into the future, including:

- The provision of a comprehensive, Commonwealth-led approach to cyber security regulation, tailored to the energy sector;
- This regulatory framework would draw on the expertise of energy sector regulators to enforce compliance, allowing existing agencies and regulators to play to their strengths;
- AEMO could play a role in establishing a technical function to assess industry compliance, if this would assist the regulator in performance of its role.

AEMO therefore supports the Government's proposal to develop a national, cross-sectoral regulatory framework, which should be informed by the work that has already been undertaken to date both in Australia and internationally, including the AESCSF and the Cyber Security Regulatory Reforms report in the energy sector.

AEMO considers that where a sector, such as the energy sector, has demonstrated a strong motivation to tackle the cyber security challenge, and has identified a pathway forward, these initiatives should be progressed, and not delayed, while a comprehensive national approach is being agreed. Efforts in the energy sector should be aligned with the overarching principles and the establishment of cross-sectorial standards as part of Australia's 2020 Cyber Strategy to enable effective harmonisation once a national approach is defined.

3. The critical role of Government

Government has unique capabilities for understanding, preventing and responding to significant and sophisticated cyber threats to Australia's national interests. Government is also uniquely positioned to drive a whole of economy approach to addressing cyber security challenges.

AEMO considers that the recommendations made in our work to date can guide the broader Government work on cyber security for the development of a whole of economy strategy. Economy wide efforts by the Government could also seek to align with the work in the energy sector so that activities can be harmonised later on.

AEMO also considers that the scale of the cyber security threat requires that resources be judiciously applied on a risk informed basis. Government has unique capabilities and influence and should seek to apply these where they can have maximum impact without replicating the efforts being made by industry. Government has a critical role to play in several key areas:

- Facilitation of collaboration between and across industry – the landscape of different sectors is becoming complex and harder to manoeuvre. It is difficult to maintain effective collaboration between a very large number of industry players in an environment of rapid transformation and increasing sector convergence;
- Drive cross-sectoral preparedness – the government can drive and monitor gaps and promote advances in preparedness to respond to critical incidences across different sectors. For example, the telecommunications sector and the electricity sector are closely related, how can both sectors respond effectively together, in the event of a cyber threat.
- Deployment of resources to areas of greatest risk including important matters such as defining and protecting critical infrastructure.
- Monitoring of potential cyber risks of new products and services coming into the markets – it is not always clear what type of cyber threat could be introduced from new technology coming onto the market. AEMO proposes to implement regulatory standards for a set of technologies that have the potential to pose cyber threats to the critical infrastructure in our economy. AEMO is happy to work with the Government to identify the types of technologies that could be considered within this category.

AEMO welcomes the opportunity to work with Government to progress the 2020 Cyber Security Strategy, and a national cyber-security regulatory regime.

ATTACHMENT 1: AEMO SUBMISSION TO Australia's 2020 Cyber Security Strategy – AEMO's answers to questions

#	Summary of questions in Cyber Security Discussion paper	AEMO's answers
Government's views		
1	What is your view of the cyber threat environment? What threats should Government be focusing on?	The cyber threat environment is increasingly hostile with a growing range of actors with the intent and capability to target and impact energy sector organisations. Sustained and focussed investments are required to keep pace with the evolving threat. AEMO agrees with the Government's view that growing cyber security is integral to ensure the security of our markets and essential services and to the physical security of energy systems in an increasingly digitised business and operational environment. Government is best positioned to focus on strategic threats to the national interest
Positioning ourselves for the future		
2	Do you agree with our understanding of who is responsible for managing cyber risks in the economy?	It is clearly a shared responsibility. AEMO believes that industry invests in people, processes and technologies to manage risks within its own sector, but partnership with Government is required to manage the cross-sectorial risks that comes with the increasing interconnectedness in the economy.
3	Do you think the way these responsibilities are currently allocated is right? What changes should we consider?	AEMO believes that the current voluntary industry activity and status quo regulation cannot adequately address the growing risk of cyber security incidents to the Australian economy, national security and communities. Because of this, AEMO appreciates that the Government is developing a nation-wide cyber security regulatory regime with a common oversight.
Government's role in a changing world		
4	What role should Government play in addressing the most serious threats to institutions and businesses located in Australia?	AEMO believes that Government should play the following roles to address cyber security risks: • Government should support and facilitate industry's understanding of sophisticated threats targeting them.

		• Government should support and facilitate the collaboration between different industry partners. • Government should drive cross-sectoral preparedness. • Government's priorities should align with the level of risk posed. • Government should monitor potential cyber risks of new products coming into the market
5	How can Government maintain trust from the Australian community when using its cyber security capabilities?	n/a
Enterprise innovation and cyber security		
6	What customer protections should apply to the security of cyber goods and services?	n/a
7	What role can Government and industry play in supporting the cyber security of consumers?	n/a
8	How can Government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings?	AEMO supports the Government's work to develop a national, cross-sectoral approach to improve the effectiveness of cyber security. The approach to cyber security should be Commonwealth-led. AEMO has already provided significant research and delivered a set of recommendations by producing the Cyber Security Regulatory Reforms Report, released in July 2019 and presented to SCO in August 2019.
9	Are there functions the Government currently performs that could be safely devolved to the private sector? What would the effect(s) be?	n/a
10	Is the regulatory environment for cyber security appropriate? Why or why not?	AEMO has produced the Cyber Security Regulatory Reforms Report, provided to the Senior Committee of Officials (SCO) of the COAG Energy Council in August 2019. This report considered the best-practice regulatory approaches to address cyber security problems in Australia's interconnected energy systems. It outlines options to implement reforms in the energy sector and formed a set of preliminary recommendations, including: • The provision of a comprehensive, Commonwealth-led approach to cyber

		security regulation, tailored to the energy sector. • This regulatory framework would draw on the expertise of energy sector regulators to enforce compliance, allowing existing agencies and regulators to play to their strengths.
11	What specific market incentives or regulatory changes should Government consider?	n/a
A trusted market place with skilled professionals		
12	What needs to be done so that cyber security is 'built in' to digital goods and services?	AEMO supports a consistent cross-sectoral standard which should be regulated at a Federal level and implemented in collaboration with industry and stakeholders.
13	How could we approach instilling better trust in ICT supply chains?	n/a
14	How can Australian governments and private entities build a market of high-quality cyber security professionals in Australia?	n/a
15	Are there any barriers currently preventing the growth of the cyber insurance market in Australia? If so, how can they be addressed?	n/a
A hostile environment for malicious cyber actors		
16	How can high-volume, low-sophistication malicious activity targeting Australia be reduced?	Mitigations at scale, as demonstrated by the UK NCSC should be considered in the Australian context.
17	What changes can Government make to create a hostile environment for malicious cyber actors?	n/a
18	How can governments and private entities better proactively identify and remediate cyber risks on essential private networks?	Proactive identification and remediation of cyber risks could be facilitated through: - Collaborative threat modelling and vulnerability analysis of proposed architectural designs for the most critical of infrastructures - Sharing of incident investigation and remediation tradecraft - Routine sharing of post incident reviews in a trusted environment - The implementation of an Australian Energy Simulation Centre would enable "what if" analysis of the consequences of malicious cyber activity, and hence improve the

		resilience of critical energy infrastructure. The US Department of Energy is embarking on a similar project: the North American Energy Resilience Model[1].
19	What private networks should be considered critical systems that need stronger cyber defences?	Recommend considering a national critical function view rather than critical asset view – see US DHS https://www.dhs.gov/cisa/national-critical-functions
20	What funding models should Government explore for any additional protections provided to the community?	n/a
21	What are the constraints to information sharing between Government and industry on cyber threats and vulnerabilities?	Over classification of information, poor understanding of where specific technologies (vulnerabilities) may be used across critical services.
A cyber-aware community		
22	To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?	n/a
23	How can an increased consumer focus on cyber security benefit Australian businesses who create cyber secure products?	n/a
24	What are examples of best practice behaviour change campaigns or measures? How did they achieve scale and how were they evaluated?	n/a
25	Would you like to see cyber security features prioritised in products and services?	n/a
26	Is there anything else that Government should consider in developing Australia's 2020 Cyber Security Strategy?	n/a

[1] DoE report available at: https://www.energy.gov/sites/prod/files/2019/07/f65/NAERM_Report_public_version_072219_508.pdf