AGL Energy Limited
T 02 9921 2999
F 02 9921 2552
agl.com.au
ABN: 74 115 061 375

Level 24, 200 George St
Sydney NSW 2000
Locked Bag 1837
St Leonards NSW 2065

Mr David Cullen

Head of Victorian Government Cyber Incident Response Service

Department of Premier and Cabinet

Submitted via email to: cybersecurity@dpc.vic.gov.au

27 October 2020

Dear Mr Cullen,

AGL welcomes the opportunity to respond to the draft State Emergency Management Plan Cyber Security Sub-Plan Edition 2 and building on the inaugural State Emergency Response Plan Cyber Security Sub-Plan released in September 2018.

AGL is one of Australia's largest integrated energy companies and the largest ASX listed owner, operator, and developer of renewable generation. AGL is also a significant retailer of energy and telecommunications, providing solutions to around 4.2 million across Australia and is the owner of some of Victoria's critical energy and generating assets.

AGL has been involved in Victoria's emergency planning and exercises for many years and AGL has comments on the following sections of the draft management plan.

Section 3.1 Emergency Management Priorities:

AGL notes that the draft plan lists the issuing of community information and warnings is a priority. AGL would add that the communication and declassification of threat data that can be used by the industry to identify indicators of compromise in a timely manner is an important aspect of this that should be explicitly stated. Clear and continuous communications to and with relevant parties within the industry (both cyber and emergency management), such as AGL is crucial in utilising industry's knowledge and experience to either prevent attacks or assist in the management of an attack or event.

Section 3.3 Mitigating cyber security risks:

AGL would suggest that the provision of advice to business and communities and mitigation strategies would be better suited to being included in guidelines to the emergency plan rather than being part of the plan itself. The mention of applicable resources in the plan e.g. The Australian Cyber Security Centre is not as useful as reproducing any relevant information in a guideline form. The guidelines could be updated regularly with the changing cyber landscape and be a more effective way to educate individuals, small business, and the community.

Within this section there should also be reference to of specific industry sector cyber frameworks or standards. For example, for financial services there is the Prudential Standard CPS234 Information Security standard and for Energy there is Australian Energy Market Operator's Australian Energy Sector Cyber Security Framework (AEMO AESCSF).

Section 3.4 Preparedness:

AGL kindly requests the creation and publication of matrix outlining responsibilities, for example a RACI matrix, in order to identify all the stakeholders involved (both government and industry), the flow of relevant information and the triggers for when the plan moves to a cross state jurisdictional model.

Section 3.4.2 Planning for cyber security emergencies & Section 3.4.5 Cyber security exercises:

AGL would recommend in addition to regular exercises undertaken, tabletop exercises be performed on a scheduled basis with industry participants to validate the plan and co-ordination points between emergency management and cyber incident response teams and departments.

3.4.3 Threat Intelligence sharing:

AGL would suggest that the communication of threat intelligence should be shared through automated channels and through a secure threat intelligence platform that organisations can subscribe to and co-ordination with the ACSC. Automation of time critical information will allow the crucial dissemination of information and assist organisations with their responsive action.

AGL requests further clarification regarding the roles and responsibilities between the sector resilience networks and the DPC roles and responsibilities with regards to cyber are unclear. For example, section 3.5.1 states that the DPC is the control agency tasked with providing advice and supporting organisations, so does that mean that the DPC will be the incident manager in the event of an attack? As mentioned above, a RACI model would assist with this clarification.

Section 3.6 Coordination and control:

AGL believes that the Figure 2 flowchart should illustrate the full lifecycle of an incident from an event to being a nationally managed incident to communicate each participants role in the lifecycle of an event. In addition, some example scenarios would assist with participant's understanding of what role each department and group play in this lifecycle.

If you would like to discuss any aspects of our response further please contact Marika Suszko, acting Regulatory Strategy Manager at msuszko@agl.com.au.

Yours sincerely,

Elizabeth Molyneux
General Manager, Policy and Energy Markets Regulation