AEMO
AUSTRALIAN ENERGY MARKET OPERATOR

2018 Summary Report into the cyber security preparedness of the National and WA Wholesale Electricity Markets

AEMO report to market participants

December 2018

Important notice

PURPOSE

AEMO has published this report pursuant to its responsibility to respond to recommendation 2.10 from the Finkel Review Report (Independent Review into the Future Security of the National Electricity Market - Blueprint for the Future - June 2017) and its broader functions to maintain and improve power system security.

DISCLAIMER

This report contains data provided by or collected from third parties, and conclusions, opinions, assumptions or forecasts that are based on that data.

AEMO has made every effort to ensure the quality of the information in this report but cannot guarantee that the information, forecasts and assumptions in it are accurate, complete or appropriate for your circumstances. This report does not include all of the information that an investor, participant or potential participant in the national electricity market might require, and does not amount to a recommendation of any investment.

Anyone proposing to use the information in this report should independently verify and check its accuracy, completeness and suitability for purpose, and obtain independent and specific advice from appropriate experts.

This document or the information in it may be subsequently updated or amended. This document does not constitute legal or business advice, and should not be relied on as a substitute for obtaining detailed advice about the National Electricity Law, the National Electricity Rules, or any other applicable laws, procedures or policies. AEMO has made every effort to ensure the quality of the information in this document but cannot guarantee its accuracy or completeness.

Accordingly, to the maximum extent permitted by law, AEMO and its officers, employees and consultants involved in the preparation of this document:

- make no representation or warranty, express or implied, as to the currency, accuracy, reliability or completeness of the information in this document; and
- are not liable (whether by reason of negligence or otherwise) for any statements, opinions, information or other matters contained or derived from this publication, or any omissions from it, or for any use or reliance on the information in it.

Executive summary

1.1 Background

Protecting the Australian electricity sector against increasingly sophisticated cyber threats is a matter of national importance - not only to ensure the integrity and reliability of electricity supply via the grid, but also for economic stability and national security purposes.

The Finkel Review Report *(Independent Review into the Future Security of the National Electricity Market - Blueprint for the Future - June 2017*[1]*)* included the following recommendation:

2.10 An annual report into the cyber security preparedness of the National Electricity Market should be developed by the Energy Security Board, in consultation with the Australian Cyber Security Centre and the Secretary of the Commonwealth Department of the Environment and Energy. The annual report should include:

2.10.1 - An assessment of the cyber maturity of all energy market participants to understand where there are vulnerabilities.

2.10.2 - A stocktake of current regulatory procedures to ensure they are sufficient to deal with any potential cyber incidents in the National Electricity Market.

2.10.3 - An assessment of the Australian Energy Market Operator's cyber security capabilities and third party testing.

2.10.4 - An update from all energy market participants on how they undertake routine testing and assessment of cyber security awareness and detection, including requirements for employee training before accessing key systems.

This is the inaugural annual report produced in response to this recommendation.

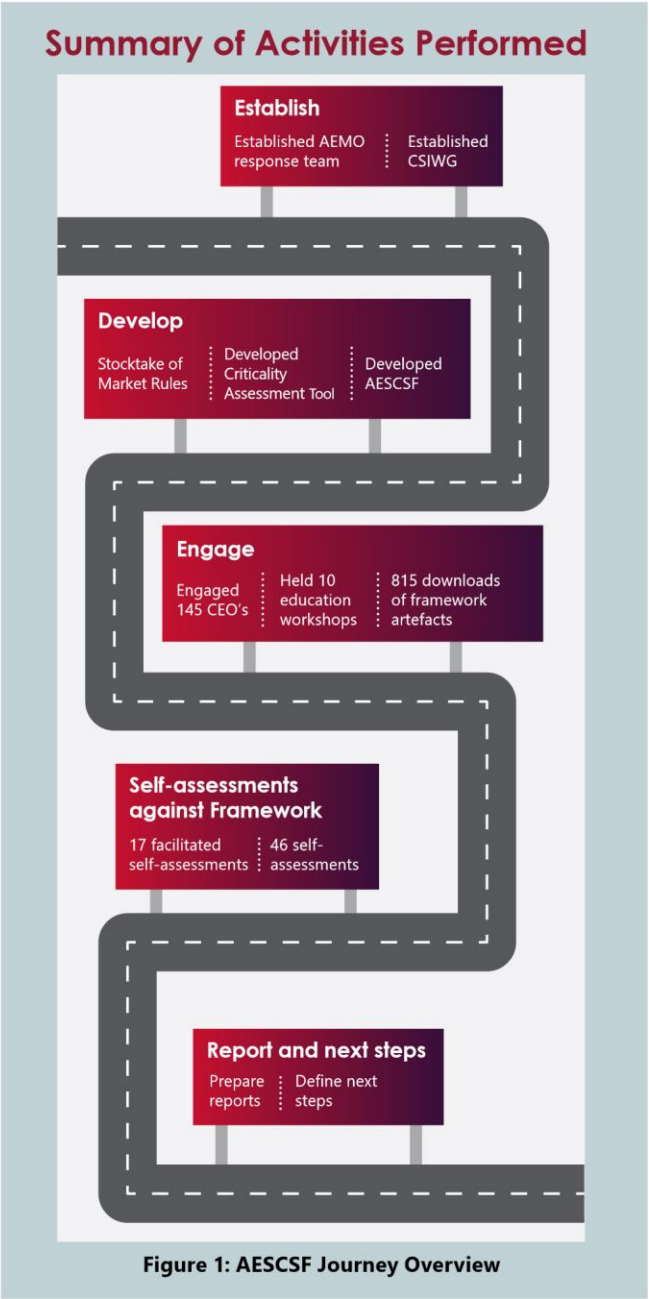

Figure 1: AESCSF Journey Overview

1.2 Summary of AEMO response

To address the evolving cyber threat landscape, and in response to Finkel Review Recommendation 2.10, the Australian Energy Market Operator (AEMO) established a program that included:

- The commissioning of a Cyber Security Industry Working Group (CSIWG) to develop a tailored cyber security framework for the Australian energy sector - now known as the Australian Energy Sector Cyber Security Framework (AESCSF).
- Consultation with parties including market participants, the Energy Security Board, Australian Cyber Security Centre (ACSC), Department of Home Affairs (DHA), Critical Infrastructure Centre (CIC), and the Secretary of the Commonwealth Department of the Environment and Energy.

Figure 1 illustrates the key activities undertaken to assess the cyber security capability maturity of the Australian electricity markets.

[1] https://www.energy.gov.au/publications/independent-review-future-security-national-electricity-market-blueprint-future

1.3 Summary of outcomes

1.3.1 A ssessment of cyber security maturity (Finkel 2.10.1)

Utilising the AESCSF, market participants across the National Electricity Market (NEM) and Western Australia Wholesale Electricity Market (WEM) were invited, for the first time, to self-assess the current state maturity of their cyber security capabilities.

AEMO and the CSIWG experienced a high level of interest and collaboration from market participants throughout this industry-wide initiative. As the completion of the self-assessment process was voluntary, and subject to a compressed time frame, the high proportion of respondents indicated a strong awareness of the importance of this subject across the sector.

145 CEOs representing entities that control 270 market participants were engaged by AEMO and the ACSC. Nominated cyber security contacts from those entities completed 67 self-assessments covering 150 market participants. 21 self-assessments were completed during workshops facilitated by AEMO for 17 high criticality and/ or regionally important entities. This response rate delivered market coverage in excess of 85% for each sub-sector in the NEM and 75%+ in the WEM.

The self-assessments completed by respondents identified opportunities to improve cyber security maturity across the sector.

1.3.2 Stocktake of current cyber security regulatory procedures (Finkel 2.10.2)

AEMO has completed a stocktake and concluded that the current provisions in the national energy regulatory framework are inadequate to address cyber security risk to the National Electricity Market. Changes to the National Electricity Law are required to extend AEMO a clear statutory function to address cyber security risks to the National Electricity Market. Any changes should also apply to the Western Australian Market and to gas under the National Gas Law.

A program of work has now commenced to determine the appropriate next steps to respond to the stocktake.

1.3.3 AEMO's cyber security capabilities (Finkel 2.10.3)

As a high criticality market participant, AEMO undertook a facilitated self-assessment of its cyber security capability maturity against the AESCSF including how it manages third party testing.

The self-assessment noted that AEMO is an industry leader with respect to cyber security information sharing and collaboration, playing a pivotal role in establishing and driving sector-wide forums and initiatives.

AEMO's self-assessment results were combined with those from the broader market participant population when responding to Finkel 2.10.1.

1.3.4 A n overview of cyber security awareness and detection practices (Finkel 2.10.4)

The AESCSF self-assessments considered how market participants raise cyber security awareness across their workforce so they can detect and report potential cyber security incidents.

Self-assessment results reported that the majority of respondents undertake cyber security awareness initiatives. Respondents reported opportunities to improve these initiatives.

1.4 Next steps

The development of the AESCSF has assisted in building collaboration and common purpose across the electricity sector in 2018 and self-assessment results have provided market participants clarity on key areas to focus and prioritise cyber security investment. This provides a strong foundation that will enable the uplift of cyber security maturity across the sector.

Having completed this initial step, a number of next steps have been identified that AEMO and the CSIWG will focus on during 2019 to continue to build on the momentum established by the framework.

Key activities include:

- Establishment of a cyber security vision for the energy sector and defining strategic goals and focus areas;
- Development of a roadmap of initiatives to collaboratively address sector-wide areas of lower maturity, for example, development of technical standards;
- Enhancement to the AESCSF based on the evolving market, cyber security threat, technology and regulatory landscapes, including alignment with Distributed Energy Resource programs;
- Consideration of potential regulatory models to strengthen AEMO's authority to manage cyber security risk;
- Improving cyber incident response preparedness through sector-wide exercises such as GridEx V in November 2019.