Australian Energy Regulator (AER)

Submitted online: ContractMarketMonitoring@aer.gov.au

Due: 20 December 2024

AER Market Monitoring Information Order MMIO-ELEC-2025-01 (the draft Order)

The Australian Energy Council ('AEC') welcomes the opportunity to make a submission to the AER's Market Monitoring Information Order MMIO-ELEC-2025-01 (the draft Order).

The Australian Energy Council is the peak industry body for electricity and downstream natural gas businesses operating in the competitive wholesale and retail energy markets. AEC members generate and sell energy to over 10 million homes and businesses and are major investors in renewable energy generation. The AEC supports reaching net-zero by 2050 as well as a 55 per cent emissions reduction target by 2035 and is committed to delivering the energy transition for the benefit of consumers.

Data security

During the consultation process for the AER's Wholesale Market Information Gathering Powers, industry was told that confidentiality and data security would be a priority for the AER and best practice would be followed. This has also been stated in the Draft Market Monitoring Information Order –MMIO-ELEC-2025-01–Explanatory Statement:[1]

> *"Our portal is routinely subjected to rigorous penetration and security testing, and documents submitted to us are stored in our official document management repository. Documents are ingested and automatically routed to the appropriate workspaces where role-based access controls can be applied to ensure data and information is accessed on a need-to-know basis. Data is encrypted both in motion and at rest."*

When using the portal, many of our members have experienced data security issues when uploading data to the AER, in contradiction of the statement above. With respect to specific details, we will leave it to individual members to detail these experiences directly with the AER. Based on members' experiences, we believe a more formal and rigorous approach needs to be adopted. Especially, when one considers the commercial sensitivity of the data. To some extent, our members are required to provide an ongoing 'data room' akin to what a serious purchaser of a business would have access to.

Some suggestions for mitigating the risk of misuse of data include:

- Stored data must be encrypted, protected from cyber theft and where possible anonymised.
- Access to data must be logged including the person that accessed it and why.
- Access strictly limited to those who need to know and provide safeguards against conflicts of interest or using the information to undertake insider trading activities for example.
- Appropriate post-engagement contractual provisions for staff and contractors with access to confidential information to protect confidentiality and, where appropriate, restrain former staff and contractors from taking commercials roles where they will be able to exploit any information during the period when the information remains commercially valuable.

Data security legislation and standards the AER could adopt

[1] Page 16.

Level 13, 575 Bourke Street
Melbourne 3000
GPO Box 1823 Melbourne Victoria 3001

P +61 3 9205 3100
E info@energycouncil.com.au
W energycouncil.com.au

ABN 92 608 495 307

The Security of Critical Infrastructure Act (2018) covers energy, data storage and processing, and financial services and markets.[2] The Wholesale Market and Reporting guidelines require our members to provide both energy and financial market data to the AER which stores and processes it. Therefore, the AER should adopt Australian Energy Sector Cyber Security Framework (AESCSF). The AESCSF:

> *"… leverages recognised industry frameworks such as the US Department of Energy's Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) and the National Institute of Standards and Technology Cyber Security Framework (NIST CSF) and references global best-practice control standards (e.g. ISO/IEC 27001, NIST SP 800-53, COBIT, etc.). The AESCSF also incorporates Australian-specific control references, such as the ACSC Essential 8 Strategies to Mitigate Cyber Security Incidents, the Australian Privacy Principles (APPs), and the Notifiable Data Breaches (NDB) scheme."*[3]

Within this framework we believe an organisation with the resources and scale of the AER, should be able to satisfy the requirements of AESCSF full assessment V2 established in 2023. Furthermore, to reassure participants we suggest that the AER engages and independent expert to audit and certify its compliance with this standard. And until this has been completed, we request that participants are not required to provide data.

The Australian Financial Markets Association (AFMA) submission covers additional topics that we have not addressed and we would like to state that we are supportive of AFMA's additional recommendations.

Finally, the AEC acknowledges that data security is an increasingly challenging undertaking and often requires more than one iteration to 'get it right' and we look forward to working collaboratively with the AER to achieve this.

Questions about this submission should be addressed to Peter Brook, by email to peter.brook@energycouncil.com.au

Yours sincerely,

Peter Brook
Wholesale Policy Manager
Australian Energy Council

[2] https://www.cisc.gov.au/information-for-your-industry
[3] https://aemo.com.au/initiatives/major-programs/cyber-security/aescsf-framework-and-resources