

Anna Collyer

Chair

Energy Security Board

Submitted via email: info@esb.org.au

ENA Response Data Strategy Initial Reforms Consultation Paper June 2022

Energy Networks Australia (ENA) welcomes the opportunity to provide input to the Energy Security Board's (ESB) Data Strategy Initial Reforms Consultation Paper June 2022.

ENA is the national industry body representing Australia's electricity transmission and distribution and gas distribution networks. Our members provide more than 16 million electricity and gas connections to almost every home and business across Australia.

Energy data held by the Australian Energy Market Operator (AEMO) has to date had very strong protections and security arrangements to ensure the privacy of each customer is protected, and to maintain the integrity of the energy market and system. ENA supports the case for increased data sharing to benefit all consumers.

However, as data sharing reforms progress, it is important the benefits from data availability to an increasing number of stakeholders is appropriately balanced against the increasing risk of cyber-attacks, data breaches and data misuse.

Key messages

- » ENA supports the intent of the reforms to open access of the existing latent data held by AEMO to trusted bodies. Data access in general should meet explicit cyber security and privacy protections requirements, be merits-based, and only be used for public good.
- » We stress the importance of securing and protecting the data. The potential harm to customers and the wider power system of cyber security attacks and/or data breaches may far outweigh the potential benefit of public good research.
 - Further protections are needed to get the balance right between data security and public benefit from data availability. Networks should provide input into the assessment process.
- » Networks should be acknowledged as Class A entities for data related to their customer base
- » The general indemnity proposed for Class A bodies should also be extended to original holders or primary sources of the data such as networks, retailers etc.
- » Strong data governance is required, including measures to ensure recipients, or their contracted parties, do not use the data for uncompetitive commercial gain or malicious intent. Governance should ensure ways to circumvent these protections are removed.
- » A thorough cost benefit assessment of the various AEMO data delivery models is needed. These options have far reaching consequences and accordingly require further engagement from stakeholders.

ENA supports increased data sharing however strong protections are required

ENA and our members support the intent of the paper, to leverage existing data in AEMO systems to drive better decisions by policymakers and produce better research outcomes that will ultimately benefit consumers. We support Class A bodies having easier and supported access to this data.

Networks currently hold and protect a significant amount of sensitive data. This includes both privacy protections under the Privacy Act and national security protections under the Security of Critical Infrastructure (SOCI) Act¹. We take significant steps to protect this data to ensure its integrity is maintained to protect customers and the power system. This data is shared with AEMO through very secure systems that adhere to strict data standards.

To ensure this data remains protected to the standards expected by the community for sensitive data, all Classes of entities obtaining data from AEMO systems should be required to meet explicit minimum levels of security (physical, cyber etc.). Third party service providers, if contracted by Class A or B bodies, should also be required to prove that they are able to meet these requirements.

ENA suggests that these security standards should be developed transparently in consultation with industry and consumer representatives. The standards should be developed with input from security experts from current data providers (such as networks and retailers) to ensure they are pragmatic and capable of practical implementation.

Data requests should be subject to merits tests

Any data sharing inherently increases the risk of data breaches, cyber-attacks and data misuse. Therefore, any request, regardless of whether it is to Class A or B bodies, should be assessed for merit and against the potential risk of harm.

ENA acknowledges that data requests are likely to range in type, granularity, sensitivity etc. quite significantly. This gives rise to different types and levels of risk. Accordingly, these factors should be taken into account by AEMO when assessing the merits of data requests.

Further, while we acknowledge that access for Class B entities, such as universities and research centres, may produce a net benefit in some instances, we believe they should be required to meet a materially higher, security and merits-based test.

Easier data access to more parties, and parties that are not bound by obligations under the SOCI Act, fundamentally increases the risk of a data breach that may have significant adverse consequences to customers, industry and the wider society. The risks are real and potentially significant. As high impact and low probability risks, they are often difficult to quantify, but should not be underestimated. These risks must be weighed against the potential benefits produced by research.

To be clear, ENA does not oppose Class B entities having access to data, but we do believe further scrutiny is warranted given the nature of the risks described above. We therefore support a rigorous, merits-based review of data access applications for entities that are not Class A or equivalent.

With regard to potential merit and costs of data requests, we consider stakeholders that are responsible for and are original sources of data, i.e. networks and retailers, should be consulted on the process by

which AEMO assesses data access requests. This is because those parties are well placed to assess whether the requested data meets the purpose of the request.

If networks and retailers are not consulted, data may be shared that is not useful to the requestor, which is likely to lead to an increase in follow-up requests to source data providers to validate the data, fill gaps etc. A large number of such requests would lead to higher resource requirements within data source providers, which adds to the overall cost of the request and the overall cost to consumers.

Networks should be Class A bodies

Networks are the source of a significant portion of the data mentioned in the paper and should therefore be considered as a Class A body. This would allow networks to access data relevant to network management which might only be available to AEMO in the future (e.g. if AEMO hold data on electric vehicle registrations per customer). This data could form valuable inputs in decisions that benefit customers, such as those related to efficient investment in and operation of the power system.

However, we do not consider that classifying networks as a Class A body should allow them access to all data sets in AEMO systems — rather it should be limited to information directly related to their customers and their networks.

Providers of source data should be indemnified

The paper proposes that Class A bodies have immunity against liability of data breach or misuse. ENA believes this also supports the need for original providers of that data to also have similar protections.

In the event of a breach by a third party, networks or other providers of ‘source’ data should not be held liable if they had no control over how the data was stored or used, or did not contribute to the breach.

Strong data governance is required

Due to the above-mentioned risks of harm with any proposed data sharing arrangements, a priority should be setting up strong data governance arrangements. This includes setting out key processes, decision makers and what requirements Class A and B bodies are required to meet.

The ESB proposes to expand the list of Class A bodies to jurisdictional energy departments. ENA supports this in principle and notes that most of these bodies operate under their own legislation, codes of conduct and regulations. A detailed assessment of these differing jurisdictional codes, especially with respect to Freedom of Information arrangements, would give networks more confidence in the secure use of the data.

ENA does not support the creation of new bodies for data sharing purposes. This will increase complexity in the process and the risk of mistakes. Rather, we propose AEMO should be responsible for assessing data requests, with a well-defined framework for requests, merits tests and security requirements.

A significant consideration for AEMO as the governing body will need to be customer protections where customers’ data is being shared with potentially a large number of commercial entities, whether as Class B bodies (including universities), or as commercial entities contracted by Class A or Class B bodies.

Further thought should be given to introducing checks and balances that ensure the data is not used for uncompetitive commercial advantage or malicious action. Equally, the data shared with parties

contracted by Class B bodies should be consistent with the information sharing restrictions between networks and their affiliated entities under ring-fencing arrangements.

ENA recommends a principles-based approach with some thought to which bodies may have enforcement and compliance powers and obligations.

We support the initial thinking around the mechanism that liability passes from AEMO to Class B bodies and would also support alternative ways that would help to close any loopholes or remove the risk of circumvention of protections.

Cost-benefit analysis of potential data provision models is needed

ENA understands that the ESB is further assessing potential data delivery models and would welcome further consultation on this issue.


Any model ultimately implemented will have wider consequences for how the cost of this service is recovered, who bears that cost, what their obligations are to stakeholders and how the data is used and protected. The trade-offs and compromises made in selecting a model for implementation should occur transparently and with adequate input from stakeholders.

Before a preferred model is selected, we consider a cost-benefit assessment is necessary, particularly in the context of significant other reforms that are increasing costs in the energy sector and to consumers. As our members bear the burden of some of AEMO's costs, it is important they are consulted on any considerations of different models.

We look forward to constructively working with the ESB, other market bodies and industry stakeholders on this issue.

If you have any questions or would like to discuss specific topics further, please do not hesitate to contact Dor Son Tan, Head of Distribution dstan@energynetworks.com.au.

Yours sincerely,



Dominic Adams

General Manager Networks

ⁱ <https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/slacip-bill-2022>