Australian Government

Department of Climate Change, Energy, the Environment and Water

Rule Change Request

Australian Energy Market Operator - Cyber Security Role

March 2024

1. REQUEST TO MAKE A RULE

1.1 Name and address of the person making the request

The Honourable Chris Bowen MP
Minister for Climate Change and Energy
Parliament House
CANBERRA ACT 2600

2. Relevant background

2.1 Energy Ministers Meeting

In December 2022, Energy Ministers endorsed the development of a National Electricity Rule (NER) change request to the Australian Energy Market Commission (AEMC) to confirm and clarify the cyber security roles and responsibilities of the Australian Energy Market Operator (AEMO)

The Department of Climate Change, Energy, the Environment and Water (DCCEEW) and AEMO have worked in consultation with jurisdictions to identify the required roles regarding cyber security for AEMO to continue meeting its obligation to improve and maintain power system security in the modern context and conferring those roles to AEMO as a minimum suite of specified cyber security functions.

2.2 Cyber Security

The energy sector needs a co-ordinated and strategic approach to effectively manage the known and increasing cyber security risk to power system security. While every sector of the economy is increasingly exposed to the risk of cyber-attacks, the energy sector is a high value target and disruptions can have serious, cascading consequences. The energy sector has a large 'attack surface' due to network connectivity and interdependencies between operational technology (OT) and information technology (IT). Russia's targeting of energy and utility assets in Ukraine, with both military and cyber attacks, are a present reminder of the importance of civil energy infrastructure to national security. Harm to Australia's interests and the interests of energy sector entities, can include economic loss such as jobs and revenue, loss of technological advantage in innovation, research and development, and intellectual property.

3. Statement of issue

3.1 Cyber security

Cyber security, while not explicitly referenced in the National Electricity Law (NEL) or National Electricity Rules (NER), has evolved rapidly as an energy security risk and is now inextricably linked with the management of the electricity and gas systems and markets. The requirements for robust cyber security risk management will continue to change quickly to adapt to new vulnerabilities, correlating closely with developments in telecommunications and digitalisation.

AEMO's role and responsibility with respect to more traditional threats to power system security is well understood and accepted by industry and government. The quickly evolving and unconventional threat posed by cyber security means AEMO's obligations for cyber security, as part of its mandate to improve and maintain power system security, is less well understood.

This rule change request seeks to establish, at minimum, a set of functions for cyber security for AEMO within the broader context of power system security. This will ensure AEMO has clear authority to deliver these functions and is resourced to support mitigation and management of

cyber security risks in the markets it manages. It will also give industry and government confidence in what to expect from AEMO in terms of supporting cyber security uplift and responding to cyber incidents or vulnerabilities which have the potential to impact energy supply.

3.2 Cyber security in the context of power system security – AEMO's role

AEMO's statutory function[1] under the NEL[2] includes the mandate to "maintain and improve power system security" (s 49(1)e). The NER provides further specificity and detail of AEMO's functions. For example, the rules add that with AEMO's function to maintain and improve power system security, AEMO has the authority to issue system security directions[3], prepare a system restart plan for managing and co-ordinating system restoration during a major disruption[4], and coordinate the protection of power system equipment[5]. Importantly, these rules detail, but do not limit, AEMO's functions described under the NEL. Similarly, the purpose of the rules proposed in this request are to provide an extra layer of detail, rather than to limit the activities which AEMO should undertake to meet its functions under the NEL.

The functions AEMO performs occur in conjunction with the security obligations of registered market participants as well as the regulatory and emergency response functions delivered under State, Territory and Commonwealth legislation, to jointly manage and respond to incidents which threaten energy supply. As per the amended *Security of Critical Infrastructure Act 2018* (SOCI Act), it is AEMO's primary responsibility to maintain the cyber security of its own assets. As the system and market operator, AEMO is uniquely placed to support the energy sector to prepare for, respond to and recover from, cyber security incidents. This directly relates to its role to improve and maintain power system security in the markets it operates.

NEM participants, government and AEMO would benefit from greater clarity within the legislative framework, acknowledging the overlap between the activities to improve and maintain power system security and cyber security management (i.e., emergency management arrangements) and the breadth of activities this could include. Without a clear allocation of agreed responsibility ownership and accountability across government and industry, cyber security efforts and capability to respond to incidents will be impacted.

4. Description of the proposed rule

This rule change request proposes to ensure AEMO can continue meeting its mandate to maintain and improve power system security in the modern context by responding to new and emerging challenges posed by the cyber security threat. In summary, the functions will enable AEMO to:

- Coordinate the system and market response to cyber incidents which impact, or potentially impact, system security and/or reliability;
- Support cyber security maturity uplift and cyber preparedness efforts led by industry;
- Provide advice to government and industry on sector-specific cyber security vulnerabilities and threats which impact, or have the potential to impact system security, where this relates to AEMO's expertise and capabilities as the system and market operator; and

[1] s49 of the NEL states (1) the following functions are conferred on AEMO: (e) to maintain and improve power system security.
[2] National Electricity (South Australia) Act 1996 | South Australian Legislation
[3] Clause 4.8.9 of the rules.
[4] Clause 4.3.1.(p)(2) and (3) of the rules.
[5] Rule 4.6 *Protection of Power System Equipment* of the rules.

- Provide, directly and by redistributing expert advice, such as from the Australian Cyber Security Centre (ACSC), critical cyber security information and advice to market participants, where the advice relates to potential risks to power system security or energy supply.

These roles are described in further detail below and in Section 6.

In order to avoid limiting AEMO's future ability to adapt to and facilitate new risks it is also important to give AEMO broad enough authority to conduct any other activity in the context of cyber security which is deemed appropriate as the market operator and system planner to improve and maintain power system security or any of its other statutory functions.

The rule change does not propose AEMO undertake any additional regulatory or compliance functions or alter existing provisions relating to AEMO's direction powers during a supply emergency. A separate process will be undertaken to examine the most appropriate pathway to replicate this rule change in the Wholesale Electricity Market (WEM)and gas markets.

4.1 Proposed cyber security functions

In addition to maintaining a high level of cyber security for its own systems and assets, AEMO and governments recognise it would be appropriate for AEMO to undertake, as a minimum, the areas of responsibilities described below.

4.2 Cyber incident coordinator

The targeted, covert and rapid escalation of cyber threats warrants early attention and intervention from AEMO and registered participants. When a cyber incident has the potential to impact energy supply, AEMO is best placed to coordinate the response of impacted market participants and jurisdictions in the event it requires the activation of any emergency protocols. Establishing and maintaining the processes for the co-ordination of cyber incident response is paramount to security of the NEM and will assist in real time management of threats as they evolve.

The proposed role will enable AEMO's enhanced coordination of the system and market response to prepare for and respond to cyber risks or incidents which threaten, or have potential to threaten, power system security and/or reliability.

For example, establishing this role as a function will allow AEMO to be adequately resourced and equipped to lead the development and stewardship of the Australian Energy Sector Cyber Incident Response Plan (AESCIRP) and implementing the plan when a cyber incident is occurring.

The AESCIRP sets out the key actions involved in the escalation from an organisational (market participant) response to a coordinated NEM cyber response and NEM operational emergency management responses. The plan establishes unique roles for AEMO including:

- the co-ordination of information during cyber incidents impacting the NEM;
- linking organisation response and management plans with those of the sectoral response plans and the Power System Emergency Response Plan (PSEMP)
- Engaging with Australian Government arrangements for cyber incident management, including for example the ACSC Cyber Incident Management Arrangements.

This role does not give AEMO the authority or obligation to manage the cyber incident response and recovery for each market participant. That remains the responsibility of each market participant, and governments in their respective jurisdictions with support from the Australian Government as required.

4.3 Supporting cyber preparedness and uplift

In similar vein to AEMO's existing efforts to improve power system security, AEMO should support cyber security uplift and cyber maturity efforts led by industry, for example as it has done through:

- Ongoing stewardship of the Australian Energy Sector Cyber Security Framework (AESCSF) and its regular assessment programs, either by its own initiative or at the request of Energy Ministers;
- AEMO developed the AESCSF with industry in response to Finkel Review recommendations.
- Supporting or undertaking the development and delivery of scenario exercises to test the cyber resilience of the electricity market;
- Participation in related groups such as the Cyber Security Industry Working Group, standards committees, and in an advisory capacity to government working groups under Energy Ministers.

Further examples of this role include:

- AEMO testing the resilience of black start procedures as part of an exercise or review.
- Providing guidance and tools for industry to improve cyber awareness and maturity, including related guidance materials, where appropriate, in partnership with relevant government agencies.

4.4 Examining risks and providing advice to government and industry

As the system and market operator for the NEM, AEMO has a unique capability to provide insights and analysis to policy makers on energy and cyber security issues.

To support this power system risk management planning and as part of AEMO's role to lead the design of Australia's future energy system, AEMO needs to have the capacity to provide, directly or as part of a coordination role, cyber security research and advice to government at all levels, where this relates to risks to the power system or market, and AEMO's expertise and capabilities as the system and market operator.

- This role leverages AEMO's unique understanding of the NEM and its associated systems and does not replace the cyber security expertise of the ACSC and other subject matter experts and authorities.
- This role may involve the preparation of specialist reports, independent advice and/or detailed analysis to be made available publicly or for a limited audience to support effective and strategic decision-making in government and industry.
- As part of the rule change, a requirement to consider prior consultation with AEMO and costs should be included.

AEMO should also be able to support or undertake the development and ongoing maintenance of cyber security standards and frameworks such as the AESCSF and promote behaviour across markets and systems as it does for other elements of energy security, to support a stronger and more effective energy system.

This would not see AEMO performing any regulatory responsibilities beyond its existing mandated scope and ability, such as its oversight for compliance with connection standards. There is no intention to impact or reduce the regulating roles of the Australian Energy Regulator (AER) or the Department of Home Affairs in relation to the SOCI Act. The examination of risk,

and the provision of advice under this provision should be separate to AEMO's responsibilities under the General Power System Risk Review (GPSRR). Providing this advice to government is essential to system security and will allow appropriate and proportionate intervention as required.

4.5 Facilitating the distribution of critical cyber security information to market participants

As the market operator, AEMO is well placed to provide, either directly or by distributing the advice of other authorities, information to warn market participants or industry of cyber security vulnerabilities or threats. For example:

- Public advisory reports, such as conclusions from the annual AESCSF assessment program, or following any significant cyber incidents on the NEM or WEM, to provide insight into the cause, response, and lessons from the event for government and industry, as it does with other events which compromise energy supply.
- The ability to provide critical cyber security information and advice to market participants, through its Market Notices system or other channels as deemed most appropriate by AEMO. This includes the notification of urgent vulnerabilities, threats, and preventative patches in commonly used digital or operational technologies to prevent the spread of malicious activity.

AEMO routinely issues notices to market participants in relation to a wide range of matters, including power system events and security, market directions, suspensions and interventions, load shedding and restoration, system re-start and general notices. Notices inform market participants of circumstances which could impact on the operation of the market security, actions AEMO is taking or expects to take, as well actions market participants might be asked to take. The benefits of AEMO redistributing cyber security advice are twofold:

- It will support AEMO's ability to maintain power system security, through the redistribution of advice which could impact reliability or registered participants through channels which industry is familiar with.
- It will assist market participants protect their own systems and take steps necessary to respond to cyber security treats.

AEMO is best placed to perform this communication role as it has an existing relationship and channel of communication with market participants. Advice coming from AEMO, even if redistributed from the ACSC or other authorities, will emphasise the importance and urgency of addressing the issues identified to market participants, and could reduce the number of different communication channels in play during a cyber incident.

5. Why the current arrangement is insufficient

AEMO is concerned the current NEL and NER are not sufficiently clear in relation to its role and responsibility for cyber security and therefore do not provide protection from liability or enable cost recovery. Clarifying AEMO's cyber security role will alleviate this concern.

To date, AEMO has performed some of these roles, as appropriate or necessary to maintain and improve power system security, in a limited capacity using existing resources. The ad-hoc nature of AEMO's engagement and lack of dedicated resourcing for the activities described above poses an ongoing risk to NEM security. As time passes without sufficient action, the risk will increase

and the ability of AEMO, government and industry to curtail these risks will become more challenging.

Changes to specify the proposed functions should be made to provide direction for AEMO to deliver the four areas of responsibilities, as per Section D, to enable AEMO to:

- Be sufficiently resourced and able to cost recover from market participants for delivering these functions; and
- Extend its protection from liability when it is delivering these functions.

Incorporating the proposed specific cyber security functions in the NER would provide AEMO, market participants and government confidence, that AEMO will deliver these functions on a consistent basis as part of its power system security responsibilities. Defining these roles will also reinforce the need for ongoing management of cyber risks and the need for strong collaboration with stakeholders to secure the markets AEMO operates.

6. Nature and scope of the proposed rule change

The proposed approach for this rule change request adds cyber security as a function in the NER. This will identify cyber security as a statutory function for the purpose for the NEL[6], enabling AEMO to apply cost recovery fees and charges[7], and confirm AEMO's immunity from liability[8] for the delivery of these services.

While this request seeks to have the specific roles outlined above defined in the rules, it is important that the roles should not be drafted in a way that limits AEMO's capability or scope to undertake other actions to manage power system security— whether cyber or by other emerging threat— evolves in the future.

This request identifies two possible locations where the new functions could be incorporated into the NER and is a matter stakeholders may wish to consider further. The first is Chapter 4, which deals with power system security, and the second is *Part D Network Planning and Expansion* of Chapter 5, which deals with network planning and expansion and includes a requirement for AEMO to undertake periodic general power system risk reviews[9].

6.1 Scope

The rule change should be sufficiently broad that it enables AEMO to undertake with certainty the responsibilities outlined in *Section C Statement of Issue,* and any other duties it deems appropriate to deliver the cyber security function in the future. Cyber security threats are a constant and evolving feature in the modern context, which requires AEMO to be dynamic in their preparation, response and recovery. The specific functions suggested for inclusion in the rule will assist AEMO to maintain power system security and inform future policy and regulatory decision to secure the NEM into the future.

The key features of the rule change would provide direction and certainty that it is appropriate for AEMO to:

1) Coordinate the system and market response to incidents that threaten system security and/or reliability, including:

[6] As per NEL 49(1)(e) AEMO's statutory function to maintain and improve power system security.
[7] NEL section 52
[8] NEL section 119
[9] NER 5.20A.

a. Development, maintenance and operation of the Australian Energy Sector Cyber Incident Response Plan;

b. Coordination and delivery of exercises to test relevant incident response plans to improve preparedness and resilience.

2) Support cyber security uplift and cyber maturity efforts led by industry, including:

a. Providing guidance and tools for industry to improve cyber awareness and maturity, including the oversight of the AESCSF and delivery of its annual assessment program.

3) Provide, directly or as part of a coordination role, cyber security research and advice to government, industry and/or the public where this relates to risks to power system security and AEMO's expertise and capabilities as the market operator and system planner.

4) Provide, directly and by redistributing advice from third-party authorities (such as from the ACSC), critical cyber security information and advice to market participants, where the advice relates to potential impacts to power system security and energy supply.

5) Undertake any other activity in the context of cyber security which is deemed appropriate by AEMO as the market operator and system planner to improve and maintain power system security or any of its other statutory functions.

6.2 Out of scope

The rule change does not propose AEMO undertake any additional regulatory or compliance functions or alter existing provisions relating to AEMO's direction powers.

Any change that could impact AEMO's existing functions that may be relevant to cyber security is out of scope. These include, for example:

- AEMO's responsibilities when it becomes aware of abnormal conditions[10] that pose an added risk to the power system;
- AEMO's Power System Security Guidelines, which specify reclassification criteria for cyber-attacks;
- AEMO's power to give *directions* to Registered Participants when necessary to maintain or re-establish the power system to a secure operating state, a satisfactory operating state, or a reliable operating state – see clause 4.8.9. These circumstances could potentially be triggered by a cyber incident affecting power system security.

While AEMO should have an expanded role to support uplift of cyber security, its role will not extend to directly managing the cyber preparedness, response or recovery outside of AEMO's own technology networks and systems. Primary responsibility for managing cyber security remains with businesses and market participants, with policy leadership provided by cyber and security agencies at all levels of government.

The rule change would not see AEMO performing any regulatory responsibilities beyond its existing mandated scope and ability, nor is there any intention to impact the regulating roles of the Australian Energy Regulator, or the Department of Home Affairs in relation to the SOCI Act.

Following this clarification for the NEM, separate processes will be undertaken to achieve clarity as to AEMO's cyber security role and responsibility in the WEM, recognising the distinct legislative and regulatory frameworks in place in Western Australia.

[10] 4.2.3 of the NER

7. How the proposed rule advances the National Electricity Objective

The National Electricity Objective (NEO), as set out in section 7 of the NEL, is:

"To promote efficient investment in, and efficient operation and use of, electricity services for the long-term interests of consumers of electricity with respect to:

- price, quality, safety and reliability and security of supply of electricity
- the reliability, safety, and security of the national electricity system.

Cyber security vulnerabilities and low cyber preparedness in the sector expose the national electricity system to safety, reliability and security risks, which could impact the price, quality, safety, reliability and security of electricity supply.

The proposed rule is in the long-term interests of consumers as it will allow AEMO to support and improve the sector's cyber security posture to defend and recover from malicious cyber incidents. This will in turn advance the reliability, safety, and security of electricity supply and the national electricity system.

8. Impact of the proposed rule on affected parties

Incorporating the proposed cyber security functions in the NER would provide confidence to AEMO, market participants and government that AEMO will be able to deliver these functions on a consistent basis as part of its power system security responsibilities. Defining these roles will also reinforce the need for ongoing management of cyber risks and the need for strong collaboration with stakeholders to secure the markets AEMO operates.

The proposal brings the following expected benefits:

- AEMO will be able to continue performing its duties with certainty, sufficient resources and immunity from liability for delivering these functions.
- Market participants would benefit from cyber uplift assistance and clear recovery protocols, including the continued development of the AESCSF and the AESCIRP.
- The improvement of cyber security preparedness across the sector reduces the risks of malicious cyber-attacks which impact energy supply, benefiting customers with improved security of supply.
- AEMO will be sufficiently resourced to advise government and industry on relevant cyber security related issues to continue to improve system security.
- The amendment will provide certainty to industry and government of AEMO's role in cyber security, in light of changing regulatory arrangements arising from the amended SOCI Act 2018 reforms.

The proposal brings the following expected costs:

- AEMO will recover costs from market participants to deliver activities specified under the rule.
- An early estimate provided by AEMO for the cost of the new functionality in line with the proposed roles would be less than $10m per annum:

	Establishment	Y1	Y2	Ongoing
Cyber Incident Coordination	4,525,000	4,250,000	3,150,000	3,125,000
Coordination of Cyber Security Research and Advice		775,000	400,000	400,000
Uplift of Cyber Security	1,560,000	2,025,000	1,525,000	1,525,000

Cyber Security Dissemination	375,000	350,000	350,000	350,000
	6,460,000	7,400,000	5,425,000	5,400,000

- The ongoing cost may change depending on the evolving cyber threat landscape and the resources required by AEMO to manage new and emerging threats accordingly over time.

9. Stakeholder Engagement

The Rule Change Request is the result of a body of work undertaken by DCCEEW and AEMO in consultation with:

- Cyber Security Working Group (now Energy Security and Resilience Working Group) under Energy Ministers, including representation from all states and territories.
- Energy Ministers

The public consultation stages within the rule change request process was identified as the best way to engage with industry on the proposed roles, approach, and outcomes.

Proposed approach to drafting the new rule

The new cyber security functions are characterised in broad terms as being necessary to preserve and enhance power system security. There are two possible locations where the new functions could be located in the NER. The first is Chapter 4, which deals with power system security, and the second is Part D of Chapter 5, which deals with network planning and expansion and includes (in rule 5.20A) a requirement for AEMO to undertake periodic general power system risk reviews. While the nature of the cyber security functions being conferred on AEMO extend beyond activities that are typically thought of as 'power system security' within the meaning of the NER, the new functions are thought to sit best in Chapter 4, and the drafting suggestions in this paper proceed on that basis. However, this is a matter which the AEMC may wish to consider further. The drafting suggestions below could readily be adapted to sit in Part D of Chapter 5 if the AEMC considers that to be a preferable location.

Purpose of Chapter 4

Clause 4.4.1 sets out the purpose of Chapter 4 – it is considered that this does not need to be amended to specifically refer to cyber security provided cyber security functions are adequately described later in the chapter.

Definition of power system security responsibilities

Clause 4.3 describes AEMO's *power system security responsibilities*. It is proposed that this rule should be expanded to include a reference in general terms to AEMO's responsibilities with respect to cyber security, and that a new sub-clause should be added later in clause 4.3 to set out those responsibilities in more detail.

This drafting approach could be achieved by inserting a new paragraph (c1) in clause 4.3.1 along the following lines (noting that the lead-in to clause 4.3.1 states 'The AEMO *power system security responsibilities* are'):

(c1) to coordinate and support cyber preparedness, response and recovery in accordance with *AEMO's cyber security functions*.

Definition of cyber security functions

The more detailed description of AEMO's cyber security functions could then be included in a new sub-clause in clause 4.3. This could possibly follow clause 4.3.2, as a new clause 4.3.2A. The drafting could be along the following lines:

4.3.2A AEMO's cyber security functions

(a) AEMO must use reasonable endeavours to coordinate the response of *Registered Participants* to a cyber incident which adversely affects or could be expected to adversely affect the secure operation of the *power system*. Without limiting the ways in which AEMO may coordinate the response, it may do so by:

(i) leading the maintenance and development of the Australian Energy Sector Cyber Incident Response Plan (AESCIRP); and

(ii) leading the implementation of the AESCIRP, in the manner provided in the AESCIRP, when a cyber incident is occurring.

(b) AEMO must use reasonable endeavours to support *Registered Participants* in improving their level of cyber security preparedness and maturity, including in collaboration with relevant government agencies and industry bodies. This may include AEMO:

(i) following consultation with *Ministers* of *participating jurisdictions*, leading the maintenance and development of the Australian Energy Sector Cyber Security Framework (AESCSF) and coordinating annual assessment programs in accordance with the AESCSF;
(ii) supporting and undertaking the development and delivery of scenario exercises to test the resilience of the *power system* to cyber threats;
(iii) developing and making available to *Registered Participants* guidance materials and tools in relation to cyber security; and
(iv) participating in working groups, standards committees and similar bodies relating to cyber security.

(c) AEMO:

(i) may, in its role as the power system and market operator, undertake research and provide advice to a *Minister* of a *participating jurisdiction* and to *Registered Participants* in relation to identified cyber security risks that may impact the power system and the management or mitigation of those risks; and
(ii) must, at the request of a Minister of a participating jurisdiction:
(A) undertake research and provide advice in relation to cyber security risks to the power system and the management or mitigation of those risks; and
(B) consult with the relevant Minister prior to undertaking the research, in relation to the nature of the research and advice being sought, AEMO's capacity and capability to undertake the research and provide the advice having regard to its role as the power system and market operator, and the likely costs that AEMO will incur in undertaking the research and advice.

(d) AEMO must use reasonable endeavours to facilitate the distribution of critical cyber security information to *participating jurisdictions* and *Registered Participants*. This may include actions such as:

(i) collating and distributing the advice of government agencies and other bodies with respect to cyber security matters relevant to the energy sector;
(ii) providing information to *participating jurisdictions* and *Registered Participants* with respect to cyber security threats and vulnerabilities of which AEMO becomes aware;
(iii) providing information to participating jurisdictions and Registered Participants with respect to preventative patches and other cyber security management and mitigations of which AEMO becomes aware; and
(iv) providing public advisory reports, including the preparation of post incident assessments to provide insights into the cause, response, and lessons learned from the incident.

Additional provisions

The rule should include a provision clarifying that these enumerated cyber security functions do not limit AEMO's existing functions that may be relevant to cyber security. These include, for example:

- AEMO's responsibilities when it becomes aware of *abnormal conditions* that pose an added risk to the power system - see clause 4.2.3A of the NER and the Power System Security Guidelines, which specify reclassification criteria for cyber attacks; and
- AEMO's power to give *directions* to Registered Participants when necessary to maintain or re-establish the power system to a secure operating state, a satisfactory operating state, or a reliable operating state – see clause 4.8.9. These circumstances could potentially be triggered by a cyber incident affecting power system security.

It should also be noted that the new cyber security functions are facilitative, in the sense that they do not confer powers on AEMO to impose mandatory obligations on Registered Participants. In particular, while the new functions envisage that AEMO may develop guidelines in relation to cyber security, such guidelines are intended to assist Registered Participants in their own cyber security preparedness and uplift efforts and are not intended to be mandatory. On that basis the new rule should clarify that any guidelines developed by AEMO under the new cyber security functions do not form part of the 'power system operating procedures' for the purpose of clause 4.10.1.