# Submission to the Australian Energy Market Commission

# National Gas Amendment (Gas cyber security roles and responsibilities for AEMO) Rule (GRC0091)

Submitted by:
Marissa McCauley
Submission made in a personal capacity

Date: 26 February 2026

---

Professional Disclaimer

This submission is provided in my personal capacity. The views expressed are my own and do not represent the views of my employer, past employers, or any affiliated organisation.

---

## Part A: Direct Responses to Consultation Questions

**Question 1: Do you consider there is a lack of clarity on the specified cyber security roles and responsibilities for AEMO in the NGR? If so, why?**

**Response:** Yes. As detailed in **Section 1** of this paper, there is a structural gap between AEMO's practical activities and its formal statutory authority. Ambiguity in "who is responsible for what" acts as a risk multiplier during high-pressure events.

---

**Question 2: Would harmonising AEMO's cyber security functions across the electricity and gas sector help to ensure a coordinated and strategic approach to cyber security risks? If so, why?**

**Response:** Yes. Due to the gas-electricity nexus, risks are cross-sectoral. As argued in **Section 3**, gas-powered generation often sets marginal prices in the NEM; therefore, a gas disruption is an electricity disruption. Harmonisation ensures AEMO has the "system-level visibility" required to manage these interdependencies.

---

**Question 3: Do you agree that the lack of funding certainty and liability protection for AEMO needs to be addressed? If so, why?**

**Response:** Yes. Funding certainty is a "resilience enabler" (see **Section 4**). Without a stable cost-recovery mechanism, institutional capability cannot be built for the long term. Liability protection is equally vital to ensure AEMO can act as a decisive "Information Clearinghouse" without the friction of litigation risk.

---

**Question 4: Would harmonising AEMO's cyber security functions across the electricity and gas sector help to ensure a coordinated and strategic approach to efficiently manage cyber security risks? Is so, why?**

**Response:** Yes. Efficiency is served by reducing "coordination latency." Data in **Section 2** shows that "breakout times" for attackers are now under 48 minutes. A harmonised framework ensures response protocols are pre-validated, which is far more efficient than ad-hoc arrangements.

---

**Question 5: Do you consider that these four functions are fit for purpose for the gas sector? Do they require any adapting?**

**Response:** These functions are fit for purpose provided they remain **risk-calibrated** (see **Section 5**). AEMO should act as a sector "integrator" rather than an operational controller, respecting the contractual nature of the gas market.

---

**Question 6: Do you consider that the benefits will outweigh the costs of the proposed solution?**

**Response:** Yes. As quantified in **Section 2**, the estimated $1.8M–$2.75M annual cost is negligible compared to the $1.2M–$3.8M **per hour** cost of infrastructure downtime. The benefits to system reliability and consumer price stability significantly outweigh the implementation costs.

---

**Question 7: Do you agree with the proposed assessment criteria?**

**Response:** I agree. However, I suggest the Commission include **"Systemic Resilience"** as an explicit lens (see **Section 5**) to evaluate how the rule strengthens the entire energy ecosystem beyond just market efficiency.

---

# Part B: Detailed Analysis

## Executive Summary

Cyber security in critical infrastructure is no longer a technical discipline operating at the periphery of market design. It is a core determinant of system reliability, investor confidence, and national resilience.

The proposal to formalise the cyber security roles of the Australian Energy Market Operator (AEMO) within the National Gas Rules (NGR) should therefore be considered not merely as a drafting clarification exercise, but as a structural governance decision.

Energy systems are increasingly digitised, interconnected and operationally interdependent. In such systems, ambiguity in accountability architecture becomes a risk multiplier.

This submission assesses the proposed amendments through a governance lens, focusing on:

- Accountability design
- Systemic coordination
- Proportional regulatory architecture
- Funding certainty as a resilience enabler
- Long-term system integrity

---

## 1. Governance Clarity and Accountability Architecture

There is currently a structural gap between AEMO's practical cyber coordination activities in the gas sector and the absence of explicit recognition within the NGR.

In complex infrastructure systems, ambiguity is not neutral. It creates:

- Hesitation in escalation
- Uncertainty in decision rights
- Fragmented response coordination
- Reduced institutional confidence

Formal recognition of AEMO's cyber functions strengthens governance clarity. It aligns statutory authority with operational reality.

From a governance design perspective, clearly defined roles reduce systemic friction during high-pressure events.

Clarity is itself a resilience mechanism.

---

## 2. Economic Rationale and Risk Quantification

To support the strategic necessity of this rule change, the Commission should consider the escalating fiscal impact of cyber-related disruptions to the Australian economy.

- **The Cost of Failure:** While AEMO's estimated costs for these functions are approximately $1.8 million to $2.75 million per annum (AEMC, 2025), the cost of inaction is significantly higher. Industry benchmarks for Australian critical infrastructure indicate that high-impact outages now cost between $1.2 million and $3.8 million per hour in lost revenue (Oxford Economics, 2025).
- **Market Volatility:** The East Coast Gas Market is highly sensitive to supply shocks. Analysis of gas market dynamics suggests that unplanned infrastructure failures can trigger regional price surges of 75% to 150% within a single trading interval (AER, 2025). Formalising AEMO's role as an "Incident Coordinator" directly mitigates "coordination latency"—the period of ambiguity that often dictates whether an incident remains contained or scales into a systemic crisis.
- **The Speed of Threat:** The transition from "informal" to "statutory" governance is necessitated by the speed of modern attacks. Notifications to Critical Infrastructure (CI) entities regarding malicious activity increased by 111% year-on-year (ASD, 2025), while the average "breakout time" (the time taken for an adversary to move laterally within a network) has dropped to just 48 minutes (CrowdStrike, 2025).

---

## 3. Systemic Coordination and Sector Interdependence

Cyber risk does not respect market boundaries.

Gas infrastructure underpins electricity generation. Electricity systems rely on gas supply during peak demand and contingency events. Digital interconnectivity further compounds cross-sector exposure.

Harmonising cyber security roles across gas and electricity markets is therefore strategically sound.

However, harmonisation must be principle-aligned — not structurally identical.

The East Coast Gas System operates differently from the centrally dispatched electricity market. The regulatory architecture should reflect:

- The contractual nature of many gas transactions
- The diversity of infrastructure ownership
- The different operational control structures

Alignment should focus on common objectives:

- Coordinated incident response
- Shared situational awareness
- Consistent escalation pathways
- Sector-wide uplift

Good governance recognises structural difference while pursuing systemic coherence.

---

## 4. Proportional Regulatory Architecture and Funding

Cyber security capability cannot be sustained through discretionary or ambiguous funding arrangements.

If AEMO is to coordinate sector-wide cyber preparedness and incident response, funding mechanisms must be:

- Transparent
- Durable
- Proportionate

Similarly, statutory immunity protections consistent with other system security functions are necessary to enable decisive action during incidents.

Underinvestment in cyber coordination capacity may reduce visible short-term cost but increases latent systemic risk.

From a governance perspective, funding certainty is not an administrative detail — it is foundational to capability maturity.

---

## 5. The Four Proposed Functions — Structuring Sector Maturity

The four proposed functions collectively establish a cyber governance scaffold for the gas sector:

1. Incident coordination
2. Preparedness and uplift
3. Risk examination and advisory
4. Information distribution

Each function contributes differently to systemic resilience.

---

## Incident Coordination

AEMO's role should be clearly defined as sector coordinator and integrator — not operational controller of participant cyber environments.

Asset owners must retain primary responsibility for their own infrastructure.

Well-defined coordination boundaries prevent:

- Role confusion
- Duplication of effort
- Escalation delays

Effective coordination reduces the duration and severity of cascading impacts.

---

## Preparedness and Uplift

Sector-wide uplift activities — scenario testing, maturity benchmarking, structured information exchange — are appropriate and forward-looking.

However, participation expectations should remain proportionate and risk-based.

Overly prescriptive obligations may impose unnecessary burden on smaller participants without proportionate resilience gains.

Strategic uplift is more effective when it is risk-calibrated.

---

## Risk Examination and Advisory

AEMO possesses system-level visibility across gas operations that individual participants do not.

This vantage point enables:

- Trend identification
- Interdependency analysis

- System-wide risk aggregation

This function should complement, not duplicate, the role of the Australian Cyber Security Centre.

Energy-specific cyber risk has unique operational characteristics. Sector-informed analysis adds material value.

---

### Information Distribution

Timely and structured dissemination of threat intelligence is critical.

Clear protocols should define:

- Escalation thresholds
- Confidentiality handling
- Integration with national reporting frameworks

Communication architecture must be deliberate. In cyber incidents, information asymmetry can exacerbate risk.

---

## 6. Efficiency Reframed — Reducing Coordination Latency

In cyber governance, efficiency should not be interpreted narrowly as cost minimisation.

True efficiency is measured by:

- Reduced coordination latency
- Clearer decision pathways
- Faster sector-wide situational awareness
- Lower probability of cascading failure

Harmonised and codified roles reduce friction during high-pressure events.

In digitally interconnected systems, speed of coordination is a primary resilience determinant.

---

## 7. Cost–Benefit Considerations

The estimated implementation costs appear proportionate relative to:

- The economic impact of a significant cyber incident

- The reputational consequences of systemic failure
- The broader national security implications

The benefits extend beyond immediate operational risk reduction. They include:

- Strengthened investor confidence
- Increased governance maturity
- Improved cross-sector trust
- Greater long-term system reliability

Periodic review mechanisms may be appropriate to ensure adaptability as threat landscapes evolve.

Cyber governance must remain dynamic.

---

## 8. Assessment Framework — Incorporating Systemic Resilience

The Commission's assessment criteria are appropriate. However, explicit recognition of systemic resilience as a decision lens would strengthen the framework.

Energy infrastructure is increasingly characterised by:

- Interdependency
- Digital integration
- Cross-sector exposure

Regulatory architecture should account for cascading risk and coordinated national response capability.

The long-term interests of consumers are inseparable from resilient infrastructure governance.

---

## 9. Conclusion

The proposed amendments represent more than clarification. They represent maturation of cyber governance within Australia's gas sector.

Formalising AEMO's cyber security functions within the NGR would:

- Align statutory authority with operational reality
- Clarify accountability architecture
- Reduce coordination friction

- Strengthen system-level resilience

Provided the rule remains proportionate, clearly bounded, and structurally tailored to the gas sector, the proposal is consistent with the long-term integrity of the East Coast Gas System.

Cyber threats will continue to evolve. Governance must evolve with them.

In critical infrastructure, resilience is not accidental.

It is designed.

###

## References:

**AEMC (2025).** *Consultation Paper: National Gas Amendment (Gas cyber security roles and responsibilities for AEMO) Rule.*

**AER (2025).** *State of the Energy Market 2025.* Australian Energy Regulator.

**ASD (2025).** *ASD Annual Cyber Threat Report 2024–2025.* Australian Signals Directorate.

**CrowdStrike (2025).** *2025 Global Threat Report.*

**IBM Security (2025).** *Cost of a Data Breach Report 2025.*

**Oxford Economics / Cyber Resilience Australia (2025).** *The Economic Impact of Infrastructure Downtime.*