# Splunk submission to AEMC on AEMO's cyber security roles and responsibilities


## Summary

Splunk is a global Data and Cloud company which provides security, analytical and performance capabilities to many of Australia's largest critical infrastructure providers, including the energy sector.

As a key security capability supplier to the Australian energy sector, Splunk has taken the opportunity to submit feedback to the Commission on the proposed rule changes to the National Electricity Rules (NER) and cyber security roles and responsibilities for the Australian Energy Market Operator's (AEMO).

Based on our unique experience and capabilities, Splunk is pleased to offer perspectives on enhancing security of Australia's power system.


## General

### Why listen to Splunk?

Leading organisations worldwide rely on Splunk for unparalleled visibility across their entire digital footprint, including Operational Technology (OT) systems. Splunk surfaces key risks and issues, empowering teams with automation to make informed decisions and respond swiftly and effectively, preventing minor issues from becoming major incidents

Splunk recognises that the energy sector underpins the Australian economy, and the industry is rapidly changing. Consumers and investors are demanding clean, reliable, and affordable sources of energy as companies contend with ageing infrastructure, changing regulations, and threats to traditional business models.

With the demand for renewable energy sources like wind and solar, market participants are focusing on infrastructure modernisation and digitisation to accommodate distributed energy

resources (DERs), improve resiliency, and drive new business models.

This transformation is producing exponential data growth and an increased cyberattack surface. Meanwhile, recruiting and retaining a new generation of talent with the necessary skills to secure and maintain IT and OT environments is a serious challenge.

Cyber maturity doesn't translate to fewer cyberattacks. However, leading organisations detect and respond faster than their peers, which softens the blow of an attack and its consequences. For incidents that caused disruption, according to Splunk's State of Security Report 2024[1], leading organisations cite a mean time to detect (MTTD) of 21 days, while developing organisations, on average, spend over a month (34 days) detecting a threat within their networks. Leading organisations also spend far less time in recovery mode. Their average mean time to recover (MTTR) business-critical workloads is just over 44 hours, while developing organisations' average recovery time is 5.7 days.

Splunks' capability brings together all data sources, including ERP systems, core infrastructure, smart meters, asset management systems, field networks and OT based systems for a single, actionable view across the entire energy value chain. With the ability to investigate, monitor and analyse large volumes of data in real time at scale, IT and business professionals are empowered to answer business-critical questions faster than ever before.

Splunk has a unique perspective into the performance and security issues facing energy providers as Splunk's capabilities are used by a large number of Australia's biggest companies, including energy operators.

Based on our capabilities and experience, Splunk's submission reflects our industry perspectives on what the national energy sector could gain by clarifying AEMO's cyber security roles and responsibilities and establishing four additional cyber security functions.

**Structure**

In this submission, Splunk is offering feedback on selected consultation questions and views on the four proposed functions in the cyber security roles and responsibilities consultation paper ("the Consultation Paper").

The remainder of this submission provides the Splunk views, and related recommendations, which are provided in two sections:

1. Stakeholder view - Splunks overall view on the proponents rule change request, including recommendations for the four additional cyber security functions
2. Question specific views - Splunks response to selected consultation papers questions

[1] https://www.splunk.com/en_us/form/state-of-security.html

## Splunk Views

**Stakeholder View**
Splunk agrees in principle with the views put forward by the proponent; Splunk believes there are benefits that the Australia power sector will realise as a result of clarifying and confirming identified cyber security roles and responsibilities to be performed by the Australian Energy Market Operator's (AEMO) enabled by explicitly referencing cyber security in the NER.

Splunk believes that explicitly referencing cyber security in the NER will add to the role that cyber security plays in operating a modern power system and the role preparedness plays in mitigating cyber security risks.

Splunk believes that the clarification and confirmation of identified cyber security roles and responsibilities, combined with requisite investment and execution of the proposed four functions will provide an opportunity for a whole-of-energy sector coordinated and programmatic cyber uplift and improved preparedness for incident coordination.

During FY2024 Splunk was directly involved with an Australian regulated sector that undertook a pilot programmatic approach to cyber uplift - enabled by a central authority. This approach utilised a repeatable methodology to enhance the sector's ability to monitor, detect and respond to cyber security events. It involved Security investigation and Event Management (SIEM) and Security Orchestration, Automated and Response (SOAR) technology, along with training for the sector's cyber workforce. The pilot achieved the following cybersecurity benefits:

- Active SIEM detections increased significantly for the majority of pilot entities enabled by an uplift of priority data sources
- Less mature entities were able to establish visibility for the majority of their ICT environment
- Confirmation that a coordinated uplift program that focuses on proactive monitoring through increased visibility, coupled with an ICT hardening program was found to be a very effective way of uplifting cyber posture across multiple sector entities.

In addition to the cyber security operational benefits, the following cost and maturity benefits were observed:

- Less mature entities deployed a foundational capability in under 4 months.
- All entities in the program avoided the costs associated with developing an organisation-specific cyber methodology.

Clarifying AEMO's roles and responsibilities - enabled by explicit cyber security referencing in the NER - and underpinned with requisite funding, will unlock potential for the power sector to achieve similar benefits to the aforementioned pilot program by enabling AEMO to better undertake cross sector preparedness and cyber uplift activities.

Splunk strongly suggests that the Commission make a decision in favour of the rule changes as proposed by the proponent. Splunks believes that making the rule changes, clarifying additional cyber security activities, and enabling the four functions with appropriate funding will directly benefit the cyber resilience of ICT and OT systems in the Australian energy sector.

To further enhance the proposed rule changes, Splunk is offering the following additional recommendations for consideration in the AEMO investment for the four identified functions:

1. AEMO's funding for the four identified functions must include capacity to encompass converged IT and Operational Technology (OT) systems to enable better coordination of sector wide incidents, more targeted cyber uplift activities and more relevant distribution of critical security information
2. AEMO's funding to provide cyber security guidance must include specific capacity to improve market participants identification of, and vulnerability management of legacy OT assets
3. AEMO's capacity to distribute and share critical cyber security information with market participants should be sufficiently funded to support rapid distribution of machine readable information for market participant security system ingestion and automation
4. AEMO's function "Supporting cyber preparedness and uplift" should include specific capacity to enable cyber skills uplift activities, including competency assessment and measurement across market participant organisations.

## Question Specific Views

**Question 1:** Do you agree that the specific cyber security activities being undertaken on an ad hoc basis is problematic?

**Answer 1: Splunk fully agrees.** Drawing on Splunk's Global industry experience, our view is that coordinated and collaborative cyber security activities are the foundation to building a cohesive approach to digital resilience, within organisations, across sectors and spanning nations.

Creating and enhancing digital resilience across the Australian energy sector is a complex but crucial task. Splunk's industry insights highlight the importance of integrating digital resilience into all aspects, from planning and product modernisation to business and product strategy, to effectively support the growth of cybersecurity maturity and culture. Achieving this goal necessitates effective coordination and collaboration.

Delivering cybersecurity activities on an ad hoc basis will not provide the needed coordination and cohesion. This lack of structure reduces the ability to effectively address evolving cyber threats and meet the cybersecurity needs of ICT and OT systems that are critical to NEM participants, further to this a consistent comprehensive cyber program will continue to build readiness within energy organisations to respond to cyber incidents.

---

**Question 2:** Do you consider there is a lack of clarity on the specified roles and responsibilities of cyber security in the NER?

**Answer 2**: **Splunk believes there is a lack of clarity and definition for cyber security and the related roles and responsibilities**. Clause 3.2.3 of the NER states that "Subject to Chapter 4, AEMO must manage the day to day operation of the power system, using its reasonable endeavours to maintain power system security in accordance with this Chapter."

Chapter 4 of the NER, outlines a number of power system security conditions, aims, principles and defines the framework for achieving and maintaining a secure power system.

Cyber security is absent from Chapter 4 (and more broadly in the NER) in definition and as a contributing factor to operating a power system in a secure operating state. Following on, the definition of cyber specific roles and responsibilities are also absent.

Cyber security considerations are a critical factor for IT and OT systems to enable secure power system operation. Splunk strongly suggests the NER is updated to clarify and define cyber security conditions, aims and principles and outlines the expected roles and responsibilities across all NEM stakeholders that participate in operating a secure power system.

**Question 3:** Would the industry value more cyber security guidance in the NER, why/why not? If yes, what kind of guidance specifically?

**Answer 3**: **Splunk suggests a targeted approach to NER specific cyber security guidance**. Splunk is not an industry organisation that operates energy systems and therefore cannot comment as an industry entity, rather Splunk is a supplier of cyber security capability to NEM industry organisations. Splunk has significant exposure and experience across a number of regulated industries around the globe and therefore believes it can provide perspectives on this question.

In the current NERs, "cyber" is mentioned once in Rule 3.7E, where it is defined in the context of an emergency or imminent cyber attack. However, with modern threats, IT systems, and sometimes OT systems that support Australia's energy systems, are constantly under cyber attack. Therefore, a broader approach is necessary, including a shift from a reactive to a proactive stance.

Splunk suggests that an increased level of cyber security guidance should be included in the NER to support all market participants, and underpins the aim of Rule 4.1 - "principles and guidance for achieving power system security".

The guidance needs to be sufficiently detailed to clearly outline expectations of AEMO and the market participants. This should include the specific roles and responsibilities of AEMO and sets expectations with market participants of what good looks like when managing cyber security risk in the sector. Splunk agrees with the suggested NER changes as defined in Section 3.1 - Solution 1a of the consultation paper.

Splunk also suggests that Rule clause 4.2.6 be updated to include a cyber security general principal clause. This will further clarify to all participants that cyber security is critical to maintaining power system security.

---

**Question 4:** Do you agree that the lack of clarity regarding the identified cyber security functions in the rules is problematic? Why or why not?

**Answer 4**: **Splunk agrees this is problematic**. If AEMO is to take a more active role in the mitigation and management of cyber security risks in the market, then the functions it performs must be defined. Clear definitions will set clear expectations for all market participants, and therefore confidence will be established.

To better enable the understanding of the NER cyber security functions, Splunks suggests that

outside of this consultation paper process, an AEMO power system cyber security strategy be developed. This would enable a strategic perspective and understanding of how legislation, NERs, AEMO activities, other strategies and relevant cyber frameworks work together to provide a cohesive approach to improving the resilience of the Australian power system and markets.

The AEMO cyber security strategy would also enable the development of an execution roadmap that encourages market consultation and participation to shape the future of the identified cyber security functions and their scope.

The AEMO cyber security strategy would afford greater transparency and collaboration, resulting in greater confidence in the market. In support of the proposed NER changes, the cyber security strategy would help further deliver on the consultations paper Solution 2 - “A strategic and coordinated approach to cyber security”.

---

**Question 5:** Do you consider cyber security a power system security issue, a network planning and expansion issue, or neither? Why/why not?

**Answer 5**: **Splunk believes that cyber security is primarily a power system security issue, but benefits could be derived in network planning and expansion**. Industry experience has shown that when best practice cyber security principles are applied at earlier stages of system and asset design and planning then risk is better managed, costs are reduced and reliability of the systems is improved.

This is reinforced by the investment made by the US CISA with Secure by Design (SbD) as the cybersecurity design concept that emphasises embedding security measures early into the planning and development phase of a product.

The most relevant example of how SbD could benefit general power system risk reviews is through the use of threat modelling. Threat modelling is the process of mapping security weaknesses in a system and prioritising how to respond to them.

Threat modelling is extremely flexible and can apply to almost any system or asset. Asset oriented threat models centre on the different components, or assets, of your system — usually ones that are attack surfaces or trust boundaries. Threat modelling can provide objective input into risk management in terms of influencing likelihood and consequence ratings.

Threat modelling can also be adapted to assist in dealing with the third-party party software and service supply chain risks. Threat models can be used with third-party software and services as part of a development process to help identify trust boundaries and relationships including where data or systems might be compromised.

AEMO could conceivably, through its cyber security functions, initiate an activity that progressively educates and introduces the use of cyber security focused threat models with network service providers. Over time, this could greatly enhance the general power system risk review. It would help prioritise risks, assess the severity of potential power system security outcomes if certain events or conditions occur, and determine the likelihood of these events or conditions happening.

---

**Question 6:** Do you consider that the benefits for clarifying the cyber security incident coordinator as a function for AEMO in the rules outweigh the costs/risks? Why/why not?

**Answer 6**: **Splunk believes that clarifying the cyber security incident coordinator as a function could outweigh the cost/risks**. Splunk believes there could be significant benefit in clarifying the cyber security incident coordinator function and programmatically enhancing and better equipping capabilities supporting the AESCIRP.

Interpreting and supporting the specific nuances of the Australian power sector as it relates to global vulnerability events is where the AEMO incident coordinator can realise significant benefits - beyond traditional cyber incident coordination. Future Solarwinds and Log4j sized events will require well-coordinated and sector specific responses due to the real likelihood of impact to power systems security and reliability.

The AEMO cyber security incident coordinator could play a pivotal role in assessing and communicating risk across the entirety of the Australian power system bridging the gap between incident, risk event and broader Government emergency management and cyber incident activities.

---

**Question 7:** Do you consider clarifying the supporting cyber preparedness and uplift as a function in the rules outweigh the costs/risks? Why/why not?

**Answer 7**: **Splunk believes that clarifying the supporting cyber preparedness as a function would outweigh the cost/risks**. Splunk believes as with most things in life, prevention is the best cure. The earlier organisations can prevent or intercept and stop an attack, the easier the remediation will be.

Therefore Splunk believes there would be significant benefit in clarifying the cyber preparedness and uplift function of AEMO, enabling greater investment in activities to coordinate and guide whole of Australian power system uplift and preparation.

As mentioned previously in this submission, Splunk was directly involved with an Australian regulated sector that undertook a pilot programmatic approach to cyber uplift - enabled by a central authority. This approach utilised a repeatable methodology to enhance the sector's

ability to monitor, detect and respond to cyber security events.

Splunk suggests that in addition to AECSF stewardship, exercise and guidance, AEMO consider the opportunity to develop campaign style initiatives that provide repeatable methodologies and coordinated expertise that tackles priority uplift areas at scale across the sector.

This will ensure that all market participants, especially those with smaller security programs, are able to gain access to pooled expertise, improve their skills and training and reduce the barrier to change and adoption of best practices.

---

**Question 8:** Do you consider the benefits of clarifying the examining risks and providing advice to government and industry as a function in the rules outweigh the costs/risks? Why/why not?

**Answer 8**: **Splunk believes that this function requires further definition before benefits can be properly considered.** Splunk strongly believes that AEMO has unique perspectives on the energy sector and they should be captured and promulgated in a manner that better informs Government, industry and market participants to make risk and investment decisions.

In answering this specific question, it is difficult for Splunk to ascertain potential benefits based on the defined scope which states advice being provided will be done so on a Ministerial request basis.

Splunk suggests that AEMO scope this function to conduct a periodic horizon scan for emerging threats, risks and capabilities specific to the energy sector. The horizon scan could be conducted on a six-monthly or yearly basis, developed in a public and non-public editions assisting all parties to understand where potential gaps in energy sector cyber risk management capabilities might exist and where future investments need to be made. The horizon scan could spin off specific research pieces that better inform stakeholders on topics of interest.

For example AI is topical in terms of the impact it has on energy systems and the potential threats and risks it introduces into the ecosystem. ENISA[2] The European Union Agency for cyber security provides a variety of informative research publications across a range of cyber security topics including some energy sector specific publications. For example, ENISA released a publication on "*CYBERSECURITY AND PRIVACY IN AI – FORECASTING DEMAND ON ELECTRICITY GRIDS*"[3] in June 2023. Example topics and papers such as this are potential perspectives that this AEMO function could provide as part of a periodic horizon scan activity.

---

[2] https://www.enisa.europa.eu/

[3]https://www.enisa.europa.eu/publications/cybersecurity-and-privacy-in-ai-forecasting-demand-on-electricity-grids

Splunk also suggests that AEMO considers that this function engages with academia and CSIRO to coordinate and where budget exists to sponsor research into cyber security specific topics that have power system or OT system relevance. The research can then be referenced and enriched by AEMO combining its own specific perspectives to better help stakeholders make more informed decisions to manage cyber risk for the Australia power system.

---

**Question 9:** Do you consider the benefits of clarifying the facilitating the distribution of cyber security information to market participants as a function in the rules outweigh the costs/risks? Why/why not?

**Answer 9**: **Splunk believes that the benefits of clarifying the facilitation of cyber security information as a function outweighs the cost/risks**. Splunk enables customers across the Globe to utilise a data-driven approach to identify, protect, detect and respond to cyber threats. Splunk's experience demonstrates where customers are able to rapidly ingest data (such as threat intelligence) and apply that to their security operations processes, then they are able to more rapidly respond to an attack and minimise the impact to their organisation.

Splunk's detailed perspective on information sharing is that sharing is substantially more effective where automation is implemented. That is, manually-based/unconnected threat intelligence sharing and response measures are unlikely to be successful as attackers move increasingly to act at machine speed, potentially aided by AI/ML.

Splunk suggests that this function could realise more benefits if AEMO implements the distribution of specific security information in a machine readable manner that enables market participants to ingest key information and intelligence in an automated manner.

## Conclusion

Splunk appreciates the opportunity to submit feedback to the Commission on the proposed rule changes to the NER and cyber security roles and responsibilities for the AEMO.

Splunk believes the suggested changes to the NER and subsequent AEMO implementation will contribute to better cyber risk management  across the Australian energy sector. Splunk also believes there is additional opportunity to increase benefits realisation of the proposed functions, and we hope the perspectives provided in this submission assist the Commission and AEMO.

Splunk believes energy is the lifeblood of modern societies, and its security is critical to the future of Australia's social, economic, political and security wellbeing.

splunk>
a CISCO company

*Nathan Smith*

Nathan Smith
Head of Security APAC
Splunk