[redacted] | Postal address [redacted] | [redacted]

5 September 2025

Department of Home Affairs
PO Box 25
Belconnen ACT 2616

Submitted by online form

Dear Mr Hansford,

Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy – Policy Discussion Paper

The Australian Energy Market Operator (AEMO) welcomes the opportunity to contribute to the consultation on Horizon 2 of the 2023–2030 Australian Cyber Security Strategy (the Strategy). As the independent electricity and gas system and market operator, AEMO plays a critical role in ensuring the reliability, security, and resilience of the national energy infrastructure.

AEMO notes the whole-of-nation approach to cyber resilience and supports the continued collaboration between government, industry, and the broader community. This submission offers targeted comments in support of the Strategy's objectives, particularly as they relate to critical infrastructure, safe technology, threat sharing, blocking, and leadership.

Protected Critical Infrastructure

AEMO supports the Strategy's emphasis on enhancing protections for critical infrastructure under Shield 4. Recent legislative reforms introduced through the *Cyber Security Act 2024* (Cth) (Cyber Security Act) and amendments to the *Security of Critical Infrastructure Act 2018* (Cth) (SOCI Act) were timely and necessary. AEMO encourages further strengthening of the Critical Infrastructure Risk Management Program (CIRMP) framework under the SOCI Act and SOCI Rules to ensure these remain adaptive to evolving threats and operational realities, in particular:

- Support for the Australian Energy Sector Cyber Security Framework (AESCSF) as the preferred energy sector-specific cyber maturity model to guide the uplift efforts across the sector, noting that most energy entities have adopted the AESCSF for their CIRMPs.
- Support consideration of energy sector entities having to meet criticality-based security profiles under the AESCSF, which is co-designed with industry and prescribed under the *SOCI (Critical Infrastructure Risk Management Program) Rules*.

The discussion paper acknowledges cyber challenges associated with emerging technologies, including distributed energy systems, and that these will need to be monitored closely, and mitigated through ongoing engagement with industry and development of proportionate, risk-based policy responses. Distributed energy systems have become a significant and increasingly prevalent feature of the National Electricity Market on the east coast and the South West Interconnected System in Western Australia. Many of these distributed energy systems are not covered by the SOCI Act (less than 30 megawatts) and similarly will not be covered by the Cyber Security Act as systems are not consumer

grade devices in place at residential and/or small business settings. The deployment of distribution energy systems in an aggregate sense, will likely need to be considered in critical infrastructure terms in the immediate term.

While recent amendments to the SOCI Act only commenced in December 2024, AEMO supports an independent review of the SOCI Act in the near term given the highly dynamic risk environment in which many critical infrastructure entities operate. It would be timely for any review to consider the CIRMP framework requirements and the scope of critical electricity assets to which SOCI obligations apply.

Safe Technology

Importantly the discussion paper identifies Consumer Energy Resources (CER) as commonly used products by Australian households where policymakers need to consider further whether existing standards provide adequate protection. CER will play a vital role in the energy transition creating a new and significant target for malicious actors.

The National CER Roadmap, endorsed by Energy and Climate Change Ministerial Council, identifies the need to establish technical standards for CER interoperability and a national technical regulatory framework, with consultation currently underway[1]. AEMO is a key industry partner to Government in the delivery of the National CER Roadmap and strongly supports both initiatives. While cyber security has been excluded from the proposed scope of the CER technical standards, the recently released National CER Roadmap Implementation Plan Update[2] introduces a new reform priority for *Cyber security for consumers and the grid (T5)* to develop a national approach for designing cyber security for CER. This work is complemented by activities under *Establish secure communication systems for CER devices (T3),* which includes the ongoing work being led by the Department of Climate Change, Energy, Environment and Water (DCCEEW) and Standards Australia to implement core elements within the roadmap for CER cyber security.

AEMO recommends that the Strategy account for National CER Roadmap reforms and any SOCI Act reforms to ensure regulatory coherence, such that there are no residual gaps and duplication is minimised.

Threat Sharing and Blocking / Strong Region and Global Leadership

The discussion paper discusses amplifying existing government and industry models for threat blocking, threat sharing, and strengthening cooperation in the region with Australia being a partner of choice. The Australian Government is in a unique position of having a whole-of-economy view into cyber security risks, being able to set policy agendas, lead diplomacy efforts with key partners (such as the Critical Five[3]) and creating opportunities for learnings. AEMO supports the Australian Government leveraging every tool at its disposal to elevate and enhance cyber security resilience.

AEMO recommends leveraging the Trusted Information Sharing Network (TISN) which is led by the Department of Home Affairs and comprises of specific critical infrastructure sectors such as energy, water, health, transport and communications. The TISN enables the sharing of information on threats, vulnerability and incidents, collaboration on the development of mitigation strategies, and the development of sector-specific resilience planning and recovery guidance. The TISN could be leveraged to facilitate multilateral sharing with global alliance partners and sector specific international peers, for example the UK's National Energy System Operator or California's Independent System Operator.

[1] National Consumer Energy Resources (CER) Roadmap - Consultation on technical priorities - Department of Climate Change, Energy, Environment and Water
[2] National Consumer Energy Resources Roadmap, Implementation Plan Update, August 2025
[3] Critical Five includes UK, USA, Canada, New Zealand and Australia

AEMO is committed to working with Government and industry partners to advance Australia's cyber resilience. We consider Horizon 2 presents a timely opportunity to consolidate gains from Horizon 1 and to embed cyber security as a foundational pillar of national infrastructure and economic strength. We look forward to participating in the next phase of co-design and implementation. Should you wish to discuss this submission further, please do not hesitate to contact [redacted], General Manager Cyber Security on [redacted]

Yours sincerely,

[redacted]

[redacted]

[redacted]