Australian Government
Department of Home Affairs

CRITICAL INFRASTRUCTURE SECURITY CENTRE

Factsheet for Critical Infrastructure

Energy Sector Technology Supply Chains

November 2025

Australia's energy sector is undergoing a monumental transformation to achieve our net-zero goals. This effort has introduced new technologies and manufacturing processes to the energy sector supply chain, which are constrained due to rising worldwide demand. This supply chain is increasingly susceptible to disruption, whether from accidental or malicious human activity or natural hazards, impacting both the development of new, and operation of existing, energy sector assets. Critical infrastructure asset owners and operators should consider the risks posed by and to their supply chain and the possible mitigations that can be implemented to limit the risk of such disruptions. This factsheet provides critical infrastructure owners and operators in the energy sector with an overview of risks to energy sector supply chains, and some risk mitigation considerations.

The energy supply chain in 2025

The energy sector transformation has required the rapid adoption of multiple technologies that are sourced and manufactured from a limited number of suppliers. Many renewable energy supply chains are consolidated in only a few countries, despite global initiatives to support supply chain diversity; China produces over 80% of completed solar panels, 70% of utility scale battery energy storage systems, and around 50-70% of wind generators. China also produces over 90% of some key renewable components.

Australia is a significant customer of the renewable energy supply chain, investing $14.1 billion in project commencements and work done in 2024. Renewables accounted for over 36% of total electricity generation Australia wide in 2024 and in FY25, rooftop solar alone accounted for 26% of installed generation capacity in the National Electricity Market (NEM).

Energy asset developers and operators are highly vulnerable to supply chain disruptions and manipulation, with possible downstream impacts on business continuity and service delivery. Disruptions to energy infrastructure may lead to economic losses, impact national resilience, social cohesion and other critical services as well as cause reputational damage for the provider.

What are the risks?

Long lead times for componentry

Projects increasingly risk delays due to supply chain constraints and high demand. In 2024, high voltage electricity transformer lead times increased from around 50 weeks to 120 weeks and lead times for large transformers, both substation power and generator step-up, ranging from 80 to 210 weeks. Should an incident occur which requires replacement components, these lead times are likely to result in disruptions that cannot be immediately rectified.

Economic coercion

Complete or near-monopolies on the provision of materials, services and supply chains significantly increase the risk of coercive activity, undermining strategic directions and goals. Monopolies can lead to a lack of pricing competition, which may allow well-placed suppliers to manipulate markets to their benefit; this could include undercutting new entrants to solidify an already dominant position or manipulating prices or cancelling exports as a means of achieving geostrategic pressure.

Russia's cut of natural gas supply to Europe in 2022 following the invasion of Ukraine, and China's restriction of exporting critical minerals to Japan in 2010, both serve as reminders of

how supply chains can be leveraged for geopolitical advantage.

Foreign disclosure laws

Some foreign governments mandate access to privately held data located within their jurisdiction, potentially including sensitive security information. Some foreign laws apply to the entirety of a company's assets, regardless of the geographic location of an asset or jurisdiction. Consequently, foreign-owned or operated companies that provide componentry or services to the electricity sector may be legally compelled to provide other governments with visibility over or access to sensitive data without the owner or operator's knowledge or consent, potentially resulting in malicious disruption. This could provide foreign governments with access, control or influence over the asset, and may simplify a malicious actor's pathway to a cyberattack, even in the absence of direct ownership.

Compromised or faulty componentry

Compromised or vulnerable components could be included during manufacture or installation, and vendor support arrangements are often implemented with remote access functionality, presenting significant additional risks and introducing vulnerabilities that can be leveraged for malicious purposes.

In May 2025, media reporting indicated that undocumented communication equipment was discovered in Chinese-manufactured solar inverters. This componentry featured additional, undocumented communication channels that could allow security controls to be remotely circumvented.

Shortage of skilled workforces

The Australian Energy Market Operator (AEMO) forecasts that the energy sector workforce is required to grow from approximately 32,000 employees to over 60,000 by 2050. The workforce uptick is required in all disciplines that interact with the energy sector, not just in engineering roles. With energy sector assets continuing to integrate smart technologies, roles such as cyber security specialists will be required in this workforce increase. The inability to fill these roles may exacerbate cyber security risks to the sector.

What can be done to mitigate these risks?

1. Supply chain resilience and expecting the worst

Businesses should consider the implications of supply chain disruption and the impacts that significant delay on delivery of componentry may have on business continuity. Considering foreign ownership, control and influence (FOCI) risks during procurement, conducting risk assessments and regularly identifying alternative vendors can uplift supply chain resilience, especially in times of increased demand. Home Affairs has released FOCI Risk Assessment Guidance to assist industry in identifying and managing technology risks where applicable to their supply chains.

2. Conduct, and act on, risk assessments

Operators of energy sector assets captured by the *Security of Critical Infrastructure Act 2018* must develop and maintain a Critical Infrastructure Risk Management Program (CIRMP) that identifies and manages material risks of hazards that could impact the asset. Supply chain is a key hazard vector under the CIRMP Hazard Rules. Businesses should conduct risk assessments, including for FOCI and cyber security risks, when selecting technology vendors and service providers, and reviewing those currently in use. Where supply chain risks are identified, they should be managed and rectified as a priority, including replacing potentially vulnerable components and service providers particularly from a provider that may attract FOCI concerns.

3. Early investment and commitment to projects

Projects may suffer delays from being "stuck" in queues for componentry and workforce expertise. Early investment can partially mitigate against supply chain risks in the future, retain Australia's spot in global queues for essential equipment and materials, and ensure that Australia's electricity network is able to respond to future market and climate events.

4. Cyber security standards and secure by design principles

As committed in the 2023-2030 Australian Cyber Security Strategy, the *Cyber Security (Security Standards for Smart Devices) Rules 2025* prescribe security standards consumer-grade smart devices and will commence on 4 March 2026. The Rules mandate security requirements to uplift the baseline cyber security across most types of consumer-grade smart devices, including household battery systems and other consumer energy resources. Adherence to these standards will assist in mitigating risks and uplift a secure by design supply chain servicing Australia.

Additional resources

SOCI obligations

Guidance for the Critical Infrastructure Risk Management Program

Australian Cyber Security Centre – Cybersecurity Guidelines

Foreign Ownership, Control or Influence Risk Assessment Guidance

Managing cyber supply chains

Critical Technology Supply Chain Principles