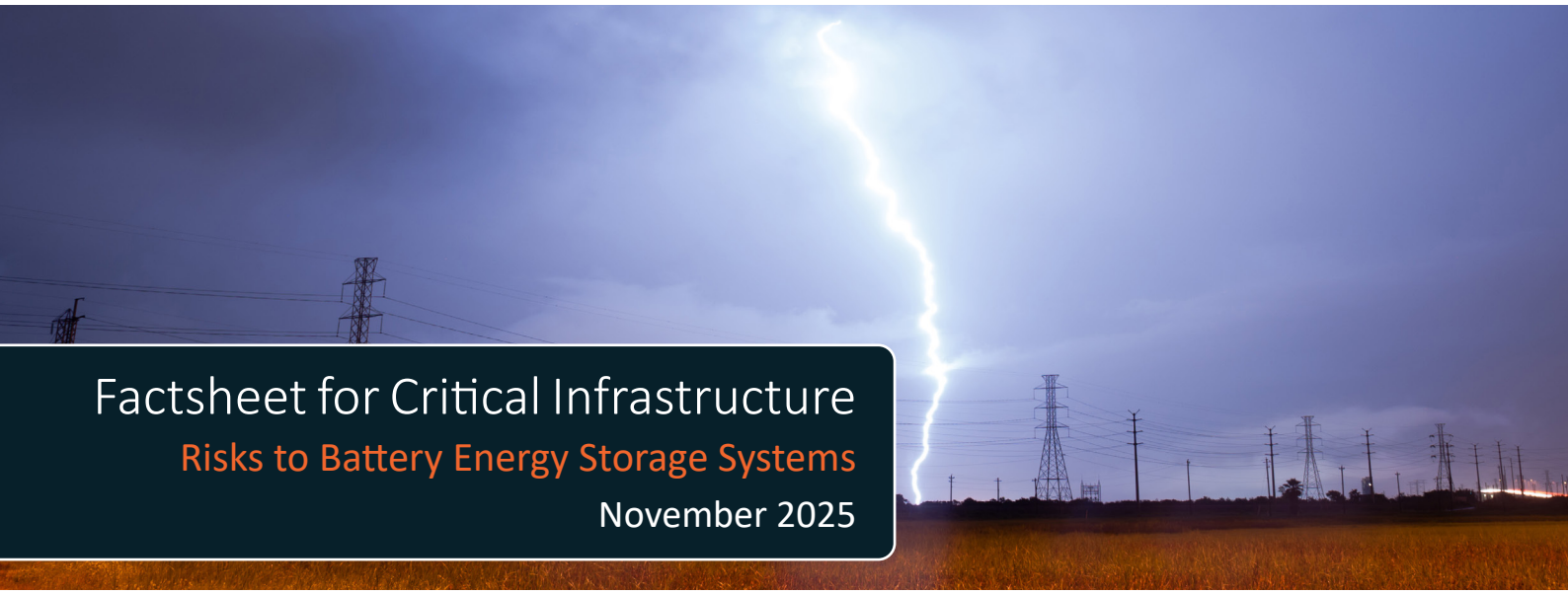
Australian Government
Department of Home Affairs

CRITICAL INFRASTRUCTURE SECURITY CENTRE



Factsheet for Critical Infrastructure

Risks to Battery Energy Storage Systems

November 2025

Utility scale battery energy storage systems (BESS)[1] play an increasingly critical role in Australia's energy transition through lowering prices, providing system reliability and stability, and supporting other sources of renewable energy. However, this criticality introduces risks, as malicious acts on BESS can have an impact on the broader electricity grid significantly larger than the capacity of the BESS. By protecting their own assets, critical infrastructure owners and operators also protect other assets which may be impacted by a cascading event. This factsheet provides an overview of BESS risk, and includes considerations for its risk mitigation.

What are Battery Energy Storage Systems?

BESS are large-scale energy storage assets that are designed to support electricity grids. BESS convert excess electricity produced in times of low demand into chemical energy, and then release this stored energy as electricity in times of increased demand.

BESS are often charged by excess renewable energy, particularly solar, and are commonly co-located with renewable energy generators and in proximity to significant transmission infrastructure corridors to improve response capabilities and efficiency.

As of July 2025, there is 2,633MW of BESS capacity operational in the National Electricity Market (NEM), with the Australian Energy Market Operator (AEMO) expecting over 9,000MW of additional BESS capacity to become operational by December 2027. BESS represent 38% of all committed, anticipated and proposed projects in the NEM

Criticality and potential impacts

BESS are increasingly critical to the stability of Australia's electricity networks as the energy transition accelerates and Australia's electricity supply becomes dominated by semi-scheduled renewable generation such as solar and wind. BESS stabilise the market and supply/demand curves during times of low supply, can provide critical Frequency Control Ancillary Services (FCAS) services to maintain system stability, and can provide System Restart Ancillary Services (SRAS) to restart a grid in the event of a system-wide outage.

Loss of these functions could lead to high and unstable pricing and prolonged blackouts. In particular, FCAS is currently provided primarily by large-scale, on-demand generators such as coal and gas-fired plants. In the event of a frequency disruption, an absence of FCAS functionality (such as that provided by BESS) can cause other energy sector assets to 'trip' and disconnect as a means of protecting themselves from physical damage, leading to significant and potentially cascading disruptions to end-users.

[1] The Department of Home Affairs considers that BESS are captured as critical electricity assets under paragraph 10(1)(b) of the *Security of Critical Infrastructure Act 2018*, provided that the entity that owns or operates it is contracted to provide a system restart ancillary service or it is an electricity generator that has an installed capacity of at least 30 megawatts, and it is connected to a wholesale electricity market (see subsection 5(1) of the *Security of Critical Infrastructure (Definitions) Rules* (LIN 21/039) 2021).

CONTACT US | enquiries@CISC.gov.au | CISC.gov.au

In addition to the risks outlined below, the commercial risks to businesses in the event of an incident are many. Incidents which impact on the wider community could lead to significant financial losses which could be compounded by reputational damage.

Key risks, threats and hazards

Cyber security risks

The Australian energy sector remains an attractive target for malicious cyber actors. As remote access and control becomes more prevalent, as well as 'always on' internet connectivity, assets become increasingly vulnerable to cyber compromise. In the absence of appropriate cyber security controls, BESS can be remotely compromised and controlled, potentially enabling espionage, sabotage, or foreign interference. Outsourcing, offshoring of data, access and control, and supply chain dependencies can exacerbate the risks.

Physical security and natural hazards

Physical attacks, shutdowns, blackouts, natural disasters can occur both onshore and offshore; however, the ability for Australian authorities to assist varies significantly across jurisdictions. Many utility scale BESS are in regional areas, relying on remote security protocols and systems. In an increasingly complex and challenging strategic environment, foreign disclosure laws and investment can exacerbate existing risks.

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 infrastructure, regardless of an asset's geographic location. Consequently, foreign-owned or operated companies, including remote and managed service providers, may be legally compelled to provide foreign governments with visibility over or access to client data without the client's knowledge or consent, or provide foreign governments with control over the asset, potentially resulting in malicious disruption. Depending on what is disclosed, allowing access to system data may make it easier for a malicious actor to undertake a cyber attack.

Foreign ownership, control and influence

If a BESS asset or its operator is subject to foreign ownership, shareholders may gain greater influence or control over company decisions, as well as visibility of sensitive security information.

When these shareholders have contrary interests to Australia's, there is an increased risk to the security of the BESS. Shareholders may maintain close links with foreign government officials or be pressured by a foreign government to undertake acts contrary to Australia's interests.

What can be done to mitigate these risks?

1. Where possible, onshore data and control

In many cases, ensuring data and control remains in Australia can be safer than allowing operations and information to be managed offshore. Where this may not be possible, businesses can reduce the risk by engaging providers that are not obligated to comply with foreign government demands.

2. Conduct, and act on, risk assessments

Where BESS assets are captured by the *Security of Critical Infrastructure Act 2018*, operators must also develop and maintain a Critical Infrastructure Risk Management Program that identifies and manages material risks of hazards that could have a relevant impact on the asset. Businesses should conduct risk assessments, including for FOCI and cyber security risks, when selecting technology vendors and service providers, and for those currently in use. This assessment is particularly pertinent when contracting data storage from a provider that may attract FOCI concerns. Where risks are identified, they should be managed and rectified as a priority, including replacing potentially vulnerable components and service providers.

3. Maintain strong cyber security hygiene

Maintaining strong cyber security controls should be a high priority for any owner or operator of a BESS. Implementing key cyber security measures can prevent many incidents and make it harder for adversaries to compromise systems or data. Ensuring employee compliance with cyber security practices will reduce opportunities for cyber breaches. Due diligence, the use of encryption, and the implementation of comprehensive risk assessment frameworks in line with Australian Government guidance can assist in mitigating national security threats.

4. Store data at secure and trusted facilities

Storing data in a location where access and security controls are clear and verifiable can mitigate risks to the integrity and availability of data. Consider both the location and FOCI of the chosen facility and the relevant jurisdictions' approach to transparency and the rule of law. Understanding the data collection laws of relevant jurisdictions will help manage data security risks that may emerge from FOCI.

Where can I find out more?

Within the Department of Home Affairs, the Critical Infrastructure Security Centre (CISC) drives an all-hazards critical infrastructure risk management regime in partnership with government, industry and the broader community. The CISC assists critical infrastructure owners and operators to understand the risk environment and meet their regulatory obligations. More information can be found on the CISC website or by contacting enquiries@CISC.gov.au.

The Critical Infrastructure Risk Management Program Guidance assists entities in understanding their obligations.

The Australian Signals Directorate provides a range of advice at cyber.gov.au to improve cyber security.

The Foreign Ownership, Control, or Influence Risk Assessment Guidance helps to manage potential risk posed by vendors operating in supply chains.