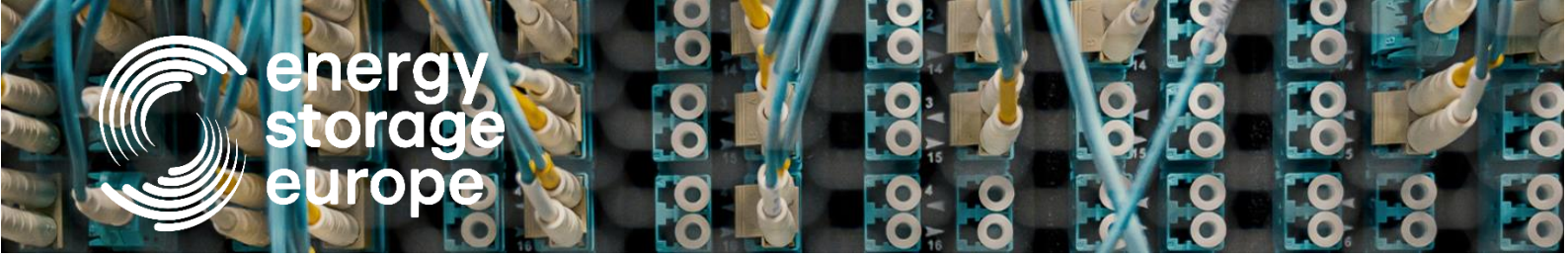

IN A NUTSHELL:

Energy Storage Europe Position on the Cybersecurity Act 2.0

Energy Storage Europe supports the Cybersecurity Act 2.0 (CSA 2.0) as the instrument to address non-technical ICT supply-chain risk and calls for targeted fine-tuning to ensure the framework is operationally precise, proportionate, harmonised across Member States, and coherent with analogous legislations, so that it strengthens grid security without fragmenting the Single Market.

Why it Matters

- The European Commission defines non-technical risk as "not from how a product is built but from who owns the supplier and what obligations its governing jurisdiction can impose on it."
- Although most mature operators restrict and monitor remote vendor access, regardless of country of origin, in some European projects, the entire control stack, BMS, EMS, PCS, and SCADA, may originate from a single non-EU provider with persistent remote access.
- The objective of strengthening European energy security and sovereignty is supported without reservation. However, this shall be achieved proportionally, and without fragmenting the Single Market.

Why this matters for the grid

Battery storage is not a "passive" product: it is technology that controls actively and in real-time the electricity system. It provides:

- Frequency response and voltage regulation
- Black start and system restoration
- Balancing and grid forming
- Sovereign grid control

The Problem and the Consequences of Inaction

The problem	Consequences if not addressed
1. "Non-technical risk" is underdefined: Article 2(39) identifies third-country suppliers but not what makes a risk high.	Suppliers may be judged solely by location rather than actual risk.
2. Technical compensating controls are not recognised: While Article 103 allows for mitigating conditions and technical controls, it remains unclear how these can be applied in practice and whether they can mitigate supplier-related risks. This creates uncertainty for asset owners and developers.	Risk-based security is weakened, as manageable risks may trigger blanket restrictions and penalise strong safety safeguards from both vendors and asset owners.
3. Member State approaches may diverge: No common criteria ensure consistent designation across the EU.	The Single Market fragments, with identical equipment potentially facing different rules across Member States.
4. Restrictions may ignore asset lifecycles: Storage projects rely on long-term contracts, multi-year systems and spare parts.	Abrupt restrictions could strand assets and disrupt contracts, maintenance and safe operation.
5. EU instruments may apply different requirements to the same suppliers and technologies: NIS2 covers supply-chain security but not ownership- and jurisdiction-based risk, which CSA 2.0 shall address.	Conflicting requirements could increase costs without necessarily improving security.

The Five Asks

1 — Define "non-technical risk" with operational precision

Adopt a legally grounded definition covering ultimate ownership and control; governing jurisdiction and state-compelled access; other jurisdictional exposure; hardware manufacturing location; software development location and team composition; software update and distribution infrastructure; cloud and data-centre jurisdiction; and insider-threat controls and corporate access policies. The definition should also specify the nature and potential impact of the risk, as well as the technical measures available to mitigate it.

2 — Give credit for technical mitigating measures

Asset owners should be able to demonstrate, through independent assessment where appropriate, that technical and organisational measures effectively mitigate identified cybersecurity risks associated with an asset. This should include risks introduced or present at the time of delivery, such as undocumented components or functionalities, as well as risks that may arise during operation.

The framework should provide clear guidance, based on the findings of the relevant risk assessment, on how such mitigating measures should be taken into account in the application of Articles 103(1) and 103(2). This would ensure that decisions appropriately reflect the residual risk of the asset and the demonstrable effectiveness of measures implemented to reduce that risk.

3 — Harmonise application across all Member States and critical sectors

Strengthening ENISA's role under CSA 2.0 is essential to ensure effective coordination, capacity building, and support for Member States and critical entities. This is particularly important given that the electricity grid operates at Union level and therefore requires a consistent approach to cybersecurity across Member States.

Cybersecurity rules should consequently be applied according to harmonised, time-bound criteria, with a meaningful right of response. Reliance on isolated national assessments risks creating regulatory fragmentation and undermining a coherent approach to cybersecurity across the Union.

4 — Mandate transition periods of at least one year

Reflect procurement and contractual lead times through risk-based, technology-specific transition periods. At least one year from the date a restriction becomes applicable should be provided for affected new procurements, with longer phase-outs for existing installations. Replacement of affected equipment or control systems in existing installations should be a last resort, taking into account asset lifecycle, technical feasibility, contractual obligations and safety.

Spare and replacement parts for existing installations should remain available for the reasonable lifecycle of the installation to ensure safe and reliable operation.

5 — Make CSA 2.0 the single reference instrument

Keep CSA coherent with the Cyber Resilience Act (CRA), including by treating critical CRA components as key ICT assets under CSA 2.0, and align NIS 2 Article 21 supply-chain risk assessments with the requirements of the CSA 2.0 framework on both technical and non-technical risk elements, ensuring that the two instruments reinforce rather than duplicate each other.

EU Industrial Accelerator Act's (IAA) financing conditions and any interim restrictions on high-risk suppliers (e.g the ones affecting high-risk inverters and PCS) should defer to the CSA 2.0 designation process rather than creating parallel or conflicting designation regimes.

What success looks like

The cybersecurity risk assessment of critical elements across the EU solar and storage value chains should assess non-technical risks and determine, for each risk category, whether and to what extent technical mitigating measures can reduce them, and where the threshold lies between technically manageable risks and risks that remain unacceptable and require supply-chain security measures.

"If NIS 2 ensures who owns the key, CRA ensures the technical requirements for the lock, and CSA ensures that the locksmith is a trusted supplier."