EU Cybersecurity Act II

Eurelectric consultation response paper

May 2026

Eurelectric consultation response to the EU Cybersecurity Act II

KEY MESSAGES

Eurelectric supports the European Commission's revision of the Cybersecurity Act and its work on harmonising cybersecurity frameworks across the Union and within the power sector. We welcome the opportunity to provide views on the revised EU Cybersecurity Act and supports its efforts to strengthen cyber resilience while improving harmonisation across the EU. In particular, we find that:

- **The designation of high-risk suppliers should be based on the combination of origin considerations based on the EU-level risk assessment and the possibility to deploy objective, transparent and verifiable mitigation measures.** The process and timeline of such designation should be clarified, alongside the launch of the union level coordinated security risk assessment.

- If a high-risk supplier is identified, the procuring entity should be given the opportunity to **demonstrate to the authorities that it can effectively mitigate** the risks through alternative appropriate technical measures. This approach would help ensure robust and efficient cybersecurity practises.

- The **proposed introduction of a transition period under the ICT supply chain framework is welcomed but must be calibrated based on the sector's procurement specificities and communicated well in advance,** given it could result in significant implementation challenges for operators. The **timeline should be extendable** and coupled with **financial coverage** due to the significant operational, financial, and system-level impacts for operators managing long-lifecycle infrastructure.

- **Transition periods should be reflected and applied in the cyber-related provisions of the IAA** to ensure consistency and alignment between the transversal legislation and sector-specific legislation.

- **Eurelectric supports the establishment of a single entry point as a first step in achieving stronger harmonisation of reporting obligations across EU legislation** (NIS2, NCCS, DORA, CRA) to reduce regulatory fragmentation, ensure interoperability, and streamline implementation. This should be followed and complemented by deeper harmonisation of reporting templates and timelines.

- **Eurelectric supports strengthening ENISA's mandate** in operational coordination, incident response, and harmonised reporting, alongside the **continued development of the ECCF and its voluntary adoption** as a tool to harmonise cyber legislation.

Eurelectric consultation response to the EU Cybersecurity Act II

Eurelectric supports efforts to align cyber legislation while strengthening the technological sovereignty of the electricity system. This is particularly important as the power sector undergoes rapid transformation to enable electrification and decarbonisation, requiring increased digitalisation amid a rising cyber threat landscape. In this context, robust cybersecurity for the European electricity sector is essential.

The ICT supply chain framework

Eurelectric welcomes the proposal and its objective of addressing non-technical ICT supply chain risks via the adoption of a risk-based approach. We recognise the importance of the Commission's effort to standardise the recognition and understanding of non-technical cyber threats at EU level via a harmonised risk assessment. In line with this spirit, we support the coordinated EU-level risk assessment, methodology to map ICT supply chains and assets at risk, and the enforcement of the mitigation measures in Article 103 (2). Nevertheless, the introduction of market-wide prohibitions, and their interactions with other cybersecurity and procurement legislation, risks bearing major implications on operators' procurement strategies and ultimately slowing down the energy transition. Eurelectric finds that a better balance should be ensured between achieving higher cybersecurity and minimising disruptions in procurement strategies that negatively affect the pace of the energy transition:

- **"High-risk suppliers" should be designated using a combination of origin considerations based on the EU-level risk assessment and the possibility to deploy objective, transparent and verifiable mitigation measures.** The process and timeline of such designation should be clarified, alongside the launch of the union level coordinated security risk assessment. Currently, it is unclear whether mitigation measures can be applied before a supplier is officially designated as high-risk. In addition, the mechanism is multi-layered and builds upon multiple implementing acts, creating system-wide uncertainty and lack of visibility.

- **Additionally, the framework should clearly identify which risks can be effectively mitigated through technical, organisational, or architectural measures, and which cannot.** This would reinforce a proportionate and risk-based approach, while supporting flexibility and resilience in electricity infrastructure.

- **Replacement periods should be extendable and accompanied by compensation for any potential disproportionate costs.** Significant implementation challenges may arise from fixed deadlines for implementing supply chain obligations, many of which may are unrealistic for operators managing highly integrated and long-lifecycle infrastructures. Requirements to replace components already deeply integrated into complex architectures, such

as the proposed three-year replacement period for Chapter II ICT supply chains, would have major impacts on long-term contracts and industrial planning. In addition, it is important to:

- Conduct comprehensive impact assessments (technical, operational, financial, and security of supply) before defining concrete replacement obligations and timelines;
- Ensure that implementation timelines are consistent with engineering realities and system stability requirements;

- **Any retroactive obligation should only be triggered by evidence-based findings** demonstrating an uncontrolled risk capable of causing serious effects on security or continuity of operations. Mitigation or phase-out measures should apply differently to new and existing projects, supported by appropriate transition periods that account for supply constraints and operational risks to electricity systems. Additionally, clear rules regarding the burden of proof should be established, including who must demonstrate non-compliance and who is responsible for implementing corrective actions.

- **Avoid duplication and inconsistent obligations between regulatory frameworks.** For example, procurement requirements part of sector-specific legislation such as the Industrial Accelerator Act should be fully aligned with cross-cutting frameworks like the CSA II to ensure clarity.

- **Clarify the definition of "ICT key assets" and the scope of ICT components.**

Incident reporting and the single entry point

Eurelectric supports the establishment of a single entry point and broader harmonisation of cybersecurity requirements to reduce fragmentation, streamline reporting, and enhance EU-level cyber resilience. This is essential to improving both operational efficiency and EU wide cyber resilience. Eurelectric recommends to:

- **Assess the possibility of using the CRA single reporting platform to support single entry point reporting**. Based on harmonised standards, this could enable interoperable and cross-framework reporting.
- **The reporting obligations in CSA II should be fully aligned with NIS2, Network Code on Cybersecurity (NCCS), DORA, and the Cyber Resilience Act to avoid overlaps**.

The European Cybersecurity Certification Framework (ECCF)

Eurelectric supports the development of the European Cybersecurity Certification Framework (ECCF) as a tool to enhance harmonisation of cybersecurity requirements and assurance practices across the EU. Eurelectric finds that:

- **Certification schemes must remain voluntary in nature, clear, stable, and aligned with real operational practices, with sufficient transition periods** to integrate requirements into existing supply chains and avoid major changes in investment signals.

- **A risk-based, proportionate approach is essential** to ensuring that certification does not create excessive administrative burdens, compliance processes, restrictions on suppliers, and significant costs. This is necessary to maintain the effective functioning of the internal market and support innovation.

Strengthening ENISA's mandate

Eurelectric supports strengthening ENISA's operational role to enhance cross-border coordination, streamline reporting, and improve cybersecurity response at EU level. We believe:

- **ENISA should lead the development of a harmonised, simplified, cross-sectoral reporting framework** that aligns NCCS, NIS2, CRA, DORA, GDPR, the Data Act, and the AI Act. This could include an ENISA-coordinated helpdesk or mechanism to ensure harmonised interpretation of compliance rules.

Eurelectric represents the interests of the electricity industry in Europe. Our work covers all major issues affecting our sector. Our members represent a total of +3500 companies in over 30 European countries.

We cover the entire industry from electricity generation and markets to distribution networks and customer issues. We also have affiliates active on several other continents and business associates from a wide variety of sectors with a direct interest in the electricity industry.

We stand for

The vision of the European power sector is to enable and sustain:
- A vibrant competitive European economy, reliably powered by clean, carbon-neutral energy
- A smart, energy efficient and truly sustainable society for all citizens of Europe

We are committed to lead a cost-effective energy transition by:

investing in clean power generation and transition-enabling solutions, to reduce emissions and actively pursue efforts to become carbon-neutral well before mid-century, taking into account different starting points and commercial availability of key transition technologies;

transforming the energy system to make it more responsive, resilient and efficient. This includes increased use of renewable energy, digitalisation, demand side response and reinforcement of grids so they can function as platforms and enablers for customers, cities and communities;

accelerating the energy transition in other economic sectors by offering competitive electricity as a transformation tool for transport, heating and industry;

embedding sustainability in all parts of our value chain and take measures to support the transformation of existing assets towards a zero carbon society;

innovating to discover the cutting-edge business models and develop the breakthrough technologies that are indispensable to allow our industry to lead this transition.

WG Sustainable Network Technology

Contact:
Jessica Garcia Moran, Policy Advisor
jgarcia@eurelectric.org
Jordan Moss, Trainee
jmoss@eurelectric.org

Union of the Electricity Industry - Eurelectric aisbl
Boulevard de l'Impératrice, 66 – bte 2 - 1000 Brussels, Belgium
Tel: + 32 2 515 10 00 - VAT: BE 0462 679 112 • www.eurelectric.org
EU Transparency Register number: 4271427696-87