

2026-05-12

The EU Cybersecurity Act - feedback

The European Solar Manufacturing Council (ESMC) welcomes the European Commission's proposal to revise the Cybersecurity Act (CSA). We strongly support the move towards a comprehensive, risk-based framework that integrates both technical and non-technical risk factors, as well as the formalisation of a high-risk supplier framework.

Europe's electricity infrastructure faces a critical and growing dependency on Chinese suppliers of inverter-based resources. Two Chinese companies control remote access to 168 GW of photovoltaic inverter capacity installed in the Union as of 2023, and around 80% of all new PV systems in Europe are installed with Chinese inverters. This concentration poses a systemic cybersecurity risk: hardware backdoors can be introduced and software as well as firmware updates can be pushed remotely, enabling simultaneous interference with millions of systems equivalent in capacity to numerous large conventional power plants. The European Commission recently has taken a first concrete step by restricting EU funding for energy projects using inverters from high-risk suppliers, citing serious economic and cybersecurity risks. Welcome as this is, guidance on funding restrictions alone is insufficient – the risk must be addressed through binding legislation at EU level. The revision of the CSA presents the right opportunity to do so. In this context, it is essential that the Trusted ICT supply chain security framework – including security risk assessment, designation of high-risk countries and ultimately prohibition of ICT components from high-risk suppliers is fully preserved.

Any weakening of the proposed ICT supply chain security framework within the CSA would undermine the Union's ability to address systemic cybersecurity risks.

ESMC strongly endorses the inclusion of criteria related to the legal and political environment of suppliers. Technical certification alone cannot mitigate risks stemming from third-country legal frameworks that requires companies to report information on software or hardware vulnerabilities to authorities of a third country prior to those vulnerabilities being known to have been exploited.

While the CSA proposal rightly addresses risks in electronic communications networks (Annex II), an equivalent level of ambition must be applied to the energy sector. Inverters for PV and battery energy storage systems, and their associated energy and battery management systems – are critical key ICT assets for inverter-based resources and thus the entire electricity system, directly contributing to grid stability, electricity generation, frequency regulation, and voltage control. At the same time, these technologies present a distinct systemic risk profile. The cybersecurity risk arises not at the level of individual installations, but from the aggregate capacity directly or indirectly

controlled by a limited number of suppliers. Hardware backdoors, firmware update systems, cloud-based platforms, and remote command interfaces create potential pathways for large-scale disruption, while the significant concentration of inverter capacity among a small number of Chinese suppliers further increases exposure to non-technical risks. Taken together, this combination creates a systemic vulnerability larger than that identified in the 5G context.

Key recommendations

1. Address cyber and supply chain security risk for inverter-based resources already in the primary legislation as is done for the ICT supply chain of communication networks.

The risk posed by inverter-based resources, including inverters for PV and battery energy storage systems, and their respective energy and battery management systems has been widely established in a multitude of independent reports and is mentioned as key example not just in the impact assessment of the CSA 2 but also in the EU economic security strategy. A respective risk assessment by the European Commission is about to be concluded. All those sources should be used to introduce articles that are mirroring the approach taken for communication networks in CSA draft articles 110 and 111. The ever-increasing concentration of the supply chain makes it a necessity to not wait for inverter-based resources-specific secondary legislation of the CSA to be adopted and implemented, which would take a lot of time. By mirroring draft articles 110 and 111 the process of phasing out of key assets from high-risk countries in inverter-based resources from the European grid could be started and communicated to the market earlier and thus create investment certainty as well as demand for trusted alternatives.

2. Introduce a new Annex IIa for key ICT assets for inverter based resources.

Those key ICT assets are: inverter hardware, software and firmware, i.e. the entire power conversion system, the energy management systems and battery management systems, firmware update and signing infrastructure, cloud-based monitoring platforms, aggregation and virtual power plant control systems and remote access and control interfaces including application programming interfaces (APIs).

Conclusion

The revision of the CSA represents a unique opportunity to align Europe's energy transition with its cybersecurity and economic security objectives. At the moment, there are sufficient trusted supplies available to meet demand in the EU market.

Manufacturers based in the EU and in likeminded countries currently hold significant inverter manufacturing capacity, and this capacity can be scaled up relatively quickly in response to policy-driven demand signals. By explicitly integrating inverter-based resources into the ICT supply chain security framework, the Union can significantly

strengthen the resilience of its future energy system. It is also an opportunity to rebuild a strategic industrial capacity at the heart of Europe's energy future.

Contact:

Jens Holm, Policy Director, ESMC

Tel: +46 708 250889, holm@esmc.solar