European Solar Manufacturing Council AISBL
2 rue de Praetere | 1000 Brussels – Belgium

ESMC fully endorses the European Commission proposal for a revised Cyber Security Act (CSA 2) and urges the co-legislators to protect the integrity of the ICT supply chain security framework, which ought to be applied to inverter-based resources in solar PV and battery technologies.

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 legislative requirements at the 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 CSA ICT supply chain security framework 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 require 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, that directly contribute 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 or accessible by a limited number of suppliers.

Hardware backdoors, firmware update systems, 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.

ESMC 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 in solar PV and battery technologies, including respective energy and battery management systems, from high-risk suppliers, has been widely established in a multitude of independent reports, was recognized by the **European Parliament** last year, and is mentioned as a key example not just in the **impact assessment of the CSA 2** but also in the **EU economic security strategy** (see list of recent and most relevant references at the end of this document). 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 connected to 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, aggregation and virtual power plant control systems and remote access and control interfaces including application programming interfaces (APIs).

Conclusion and take-aways:

The revision of the CSA represents a unique opportunity to align Europe's energy transition with its cybersecurity and economic security objectives on top of preserving tens of thousands of high-quality industrial and R&D jobs mainly in Spain, Germany, Austria but also in the Czech Republic, France and Italy.

By explicitly integrating inverter-based resources into the ICT supply chain security framework the Union would not slow down the energy transition.

European and other Western manufacturers currently – still – have the capacity to meet all of EU demand. Many of those capacities are currently being under-utilized because industrial overcapacities are being dumped in the EU market. The supply chain is dramatically concentrating.

Independent research shows that the cost increase of using trustworthy key ICT assets for inverter-based resources would increase overall project CAPEX in the utility-scale and C&I segment by ~2%, and ~4% in the residential segment. The effect on LCOE would de facto be negligible.

The proposed amendments below are chosen so that no new key ICT assets for inverter-based resources from high-risk suppliers are connected to the EU electricity grid after the adoption of the CSA. For phasing out existing ICT components from Key ICT assets for inverter-based resources in solar PV and battery technologies the Commission needs to decide a timeline that is proportionate to the risk but balanced, safeguarding as much as possible investment security for existing assets. The life span of an inverter, depending on the use case, is normally between 8 and 12 years.

European Solar Manufacturing Council AISBL
2 rue de Praetere | 1000 Brussels – Belgium

ESMC

AMENDMENTS TO

Proposal for a Regulation of the European Parliament and of the Council

on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881

(The Cybersecurity Act 2)

COM(2026) 11 final — 2026/0011(COD)

Subject: ICT Supply Chain Security of Inverter-Based Resources

Explanatory Note

These amendments use Articles 110–111 and Annex II (the 5G/telecom provisions) as their direct structural and linguistic template. The same legislative logic that justified mandatory restrictions for high-risk suppliers from 5G infrastructure applies with equal force to inverter-based resources: systemic grid risk, high and increasing concentration of supply from a single third country, and the absence of effective judicial remedies against state-compelled supplier cooperation in that third country. The amendments are framed under Article 114 TFEU (internal market) and are consistent with recital (133), which already lists 'electricity supply systems and electricity storage' among the supply chains at risk.

Format: Additions to existing text and entirely new provisions are shown in bold and italic.

European Solar Manufacturing Council AISBL
2 rue de Praetere | 1000 Brussels – Belgium

Provision	Text as proposed by the Commission (COM(2026) 11 final)	Amendment (Additions in bold & italic)
Amendment 1 | New Recital (133a) — *PV inverters as systemic ICT supply chain risk — legislative grounding*		
New Recital (133a) *Insert after Recital (133)*	*(No existing text — new provision)* **Current Recital (133) reads:** Cybersecurity risks, including risks related to dependency on high-risk suppliers may be observed in several critical ICT supply chains in the Union, including detection equipment, connected and automated vehicles, electricity supply systems and electricity storage, water supply systems, drones and counter-drones systems, cloud computing services, medical devices, surveillance equipment, space services and semiconductors. For example, vulnerabilities in security detection equipment could grant access to ICT systems allowing malicious actors to manipulate scanners in such a way that prohibited items could be brought through the security checkpoint without being detected, with possibly catastrophic consequences.	*(Insert new Recital (133a) after existing Recital (133)):* ***New Recital (133a):*** ***The ICT supply chain framework established by this Regulation should apply to key ICT assets for inverter-based resources in solar PV and battery technologies. They are directly contributing to energy generation and storage, grid stability, frequency regulation and voltage control, yet their supply chain is increasingly concentrated. Potential backdoors as well as standard remote access capabilities, including firmware update channels and virtual power plant control systems represent a systemic attack surface giving rise to strategic dependencies that pose risks to the security and continuity of the Union's electricity supply. No key ICT assets for inverter-based resources from high-risk suppliers subject to a jurisdiction of a country that poses a cyber security risk to the Union should be connected to the EU electricity grid.***
Justification The Commission's own Impact Assessment (SWD(2026) 11, Section 2.2.3, Driver 3) identifies PV inverter supply chains as an illustrative case of the non-technical risk justifying this Regulation, noting that 225 GW (64%) of European inverter shipments 2015–2023 came from Chinese companies, that two Chinese vendors control remote access to 168 GW of EU PV capacity as of 2023 and that 150+ Chinese-authored publications are simulating EU grid disruptions. This recital gives legislative expression to that Commission problem definition. By anchoring the new recital after Recital 133 — which already lists "electricity supply systems and electricity storage" — the amendment stays within the established legislative architecture and provides the recital basis required for the new operative provisions proposed below.		

European Solar Manufacturing Council AISBL
2 rue de Praetere | 1000 Brussels – Belgium

Provision	Text as proposed by the Commission (COM(2026) 11 final)	Amendment (Additions in bold & italic)
Amendment 2 | Article 98 — new paragraph 4 — *Scope extension: aggregate-capacity risk assessment for inverter-based resources*		
Article 98 New paragraph 4 *Scope of the framework*	1. The trusted ICT supply chain framework shall provide for a security mechanism at Union level to address non-technical risks in sectors of high criticality and other critical sectors as referred to in Directive (EU) 2022/2555. The mechanism shall identify key ICT assets in critical ICT supply chains and set out appropriate and proportionate mitigation measures on entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555. 2. The obligations set out in this Title shall be without prejudice to obligations set out in Article 13 of Regulation (EU) 2024/2847 and in national provisions transposing Article 21 of Directive (EU) 2022/2555. 3. The provisions laid down in this Chapter shall not preclude Member States from adopting or maintaining provisions ensuring a higher level of cybersecurity in ICT supply chains, provided that such provisions are consistent with their obligations under Union law.	1. The trusted ICT supply chain framework shall provide for a security mechanism at Union level to address non-technical risks in sectors of high criticality and other critical sectors as referred to in Directive (EU) 2022/2555. The mechanism shall identify key ICT assets in critical ICT supply chains and set out appropriate and proportionate mitigation measures on entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555. 2. The obligations set out in this Title shall be without prejudice to obligations set out in Article 13 of Regulation (EU) 2024/2847 and in national provisions transposing Article 21 of Directive (EU) 2022/2555. 3. The provisions laid down in this Chapter shall not preclude Member States from adopting or maintaining provisions ensuring a higher level of cybersecurity in ICT supply chains, provided that such provisions are consistent with their obligations under Union law. ***4. For the purposes of applying the framework established by this chapter to key ICT assets for inverter-based resources in solar PV and battery technologies, the determination of systemic risk to electricity grid stability shall be based on the aggregate capacity and impact of such resources whose key ICT assets are supplied, directly or indirectly controlled or accessible by a single supplier irrespective of whether individual owners or operators of such inverter-based resources qualify as entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555.***

Justification

Article 98(1) currently limits the framework's mitigation measures to 'entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555'. This creates a structural gap for PV inverters: individual residential and commercial owners fall below NIS2 thresholds as long as they are not aggregated by an 'entity of the type referred to in Annexes I and II to Directive (EU) 2022/2555'. The risk is not at the individual device level but at the supplier-concentration level. This amendment closes the aggregation gap by establishing that the systemic risk assessment unit for inverter-based resources is aggregate per-supplier capacity, not individual system size. It preserves the architecture of Art. 98 while extending it to cover the specific topology of distributed energy resources.

Provision	Text as proposed by the Commission (COM(2026) 11 final)	Amendment (Additions in bold & italic)
Amendment 3 | New Chapter IIa — Articles 111a & 111b — *Prohibition and mandatory phase-out of key ICT assets for inverter-based resources from high-risk suppliers (modelled on Arts. 110–111)*		
New Chapter IIa ***New Article 111a*** ***New Article 111b*** *Insert after Article 111* *(i.e. after existing Chapter II on telecom networks)*	*(No existing text — new Chapter and Articles)* **For reference, the analogous provisions for electronic communications networks are:** Article 110(1): 'The key ICT assets for mobile, fixed and satellite electronic communications networks shall be as set out in Annex II.' Article 110(2): 'ICT components [...] provided by high-risk suppliers shall be phased out from the key ICT assets of mobile, fixed and satellite electronic communication networks.' Article 110(3): '...shall not exceed 36 months from the publication of the list of high-risk suppliers...' Article 111(1): 'Providers of mobile, fixed and satellite electronic communications networks shall not use, install or integrate, in any form, ICT components [...] from high-risk suppliers in the operation of key ICT assets referred to in Annex II.'	***CHAPTER IIa ICT SUPPLY CHAINS IN INVERTER-BASED RESOURCES*** ***Article 111a*** ***Key ICT assets for inverter-based resources in solar PV and battery technologies:*** ***1. The key ICT assets for inverter-based resources shall be as set out in Annex IIa.*** ***2. No new inverter-based resources that include key ICT assets, referred to in Annex IIa, from high-risk suppliers subject to a jurisdiction of a third country posing cybersecurity concerns shall be connected to the EU electricity grid after the date of entry into force of this act.*** ***3. ICT components or components that include ICT components provided by high-risk suppliers subject to a jurisdiction of a third country posing cybersecurity concerns that have been installed before the entry into force of this act shall be phased out from key ICT assets of inverter-based resources referred to in Annex IIa.*** ***4. The Commission is empowered to adopt implementing acts in accordance with Article 118(2) to specify the time periods for the phasing out the ICT components or components that include ICT components from high-risk suppliers subject to a jurisdiction of a third country posing cybersecurity concerns***

Provision	Text as proposed by the Commission (COM(2026) 11 final)	Amendment (Additions in bold & italic)
		for key ICT assets of inverter-based resources referred to in Annex IIa. ***5. The Commission is empowered to adopt delegated acts in accordance with Article 119 to amend Annex IIa to this Regulation in order to adapt it to technological developments by taking into account the elements referred to in Article 103(4) and the results of risk assessments conducted pursuant to Article 99(5).*** ***Article 111b*** ***Prohibitions for inverter-based resources*** ***1. Entities listed for the electricity sector in Annex 1 of Directive 2022/2555 shall not use, install, or integrate, in any form, ICT components or components that include ICT components from high-risk suppliers in the operation of key ICT assets referred to in Annex IIa.*** ***2. Transmission system operators and distribution system operators as defined in Article 2 of Directive 2019/944 shall refuse connection and, if relevant registration, of new inverter-based resources, irrespective of system size, that include ICT components or ICT components that include ICT components from high-risk suppliers in the operation of key ICT assets referred to in Annex IIa.***

Justification

Articles 110–111 establish the paradigm for sector-specific application of the trusted ICT supply chain framework to electronic communications networks (5G). They provide the direct legislative template for this amendment. The structural parallels are exact: inverter-based resources play the same systemic grid role as 5G networks play in the communications ecosystem, both in terms of criticality and in terms of the concentration of supply from high-risk third countries. The proposed amendments are chosen so that no new key ICT assets for inverter-based resources from high-risk suppliers are connected to the EU electricity grid after the adoption of the CSA. New articles 111a (2) and 111b (2) are crucial to also ensure the inclusion of the residential and small commercial market segment. In case registration with the DSO is required new article 111b (2) would also include plug-in systems. An additional connection of chapter IIa with the CRA could also be considered. For phasing out existing ICT components from key ICT assets as specified in Annex IIa the Commission needs to decide a timeline that is proportionate to the risk but balanced, safeguarding as much as possible investment security for existing assets. The life span of an inverter, depending on the use case, is normally between 8 and 12 years.

Provision	Text as proposed by the Commission (COM(2026) 11 final)	Amendment (Additions in bold & italic)
Amendment 4 | New Annex IIa — *Key ICT assets for inverter-based resources (modelled on Annex II)*		
New Annex IIa *Insert after Annex II* *Referenced in Arts. 110a and 110b*	*(No existing text — new Annex)* **For reference, Annex II defines key ICT assets for electronic communications networks by reference to defined terms in Art. 2, covering:** • Core network functions of mobile networks (Art. 2(44)) • NFV/MANO of mobile networks (Art. 2(45)) • Radio access network (RAN) (Art. 2(46)) • Core network functions of fixed networks (Art. 2(47)) • Network management system of fixed networks (Art. 2(48)) • Transport and transmission functions of fixed networks (Art. 2(49)) • Access network of fixed networks (Art. 2(50))	***ANNEX IIa*** ***Key ICT assets for inverter-based resources in solar PV and battery technologies*** ***The following shall constitute key ICT assets for inverter-based resources in solar PV and battery technologies for the purposes of this Regulation:*** ***1. The inverter in solar PV and battery technologies (Art. 2 (new))*** ***2. Energy and battery management systems (Art. 2 (new))*** ***3. Firmware and software update and signing infrastructure (Art. 2 (new))*** ***4. Remote access and command interfaces including application programming interfaces (APIs) (Art. 2 (new))*** ***5. Aggregation and virtual power plant (VPP) control systems (Art. 2 (new))***

Justification

Annex IIa mirrors the structure and granularity of Annex II (telecom key ICT assets), which uses defined terms in Art. 2 to specify the exact asset classes covered. The 5 assets in Annex IIa are designed to be technologically precise, future-proof and coherent with the existing cybersecurity literature on inverter attack surfaces. The 5 assets together correspond to the core attack vector identified by DNV/SolarPower Europe, NUKIB, BSI and the Forescout SUN:DOWN reports and other reports referenced down below.

The amendments are fully justified based on i.a. the following reports:

1.) European Parliament resolution of 8 July 2025 on the security of energy supply in the EU (2025/2055(INI)), paragraph 27 & 28: https://www.europarl.europa.eu/doceo/document/TA-10-2025-0146_EN.pdf

2.) IMPACT ASSESSMENT REPORT Accompanying the documents Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2), SWD(2026) 11 final, pages 29 & 30: Register of Commission Documents - SWD(2026)11

3.) JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Strengthening EU economic security, JOIN(2025) 977 final, pages 11 & 12: eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025JC0977

4.) NATO ENERGY SECURITY CENTRE OF EXCELLENCE, Highly Decentralized and Intelligent Power Systems - Risks and Opportunities for Energy Security, pages 19-22: https://www.enseccoe.org/wp-content/uploads/2026/01/Energy-Highlights-No.21_A4_single-page.pdf

5.) Czech National Cyber and Information Security Agency (NUKIB), WARNING: https://nukib.gov.cz/download/publications_en/EN_2025-09-03_warning.pdf

6.) German Federal Office of Information Security (BSI), Positionspapier: Cybersicherheit im Energiesektor Deutschlands: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Positionspapier_Cybersicherheit_Energiesektor.pdf?__blob=publicationFile&v=2

7.) European Union Institute for Security Studies (EUISS): The dragon in the grid: Limiting China's influence in Europe's energy system: https://www.iss.europa.eu/publications/briefs/dragon-grid-limiting-chinas-influence-europes-energy-system

8.) SolarPower Europe/DNV, see i.a. pages 33 & 34 as well as 40 & 41: SPE_2025_Solutions_for_PV_Cyber_Risks_to_Grid_Stability_032dc2ae5a.pdf

9.) Forescout: SUN:DOWN Vulnerability Research Report - Forescout

10.) Strider: Strider-Report-In-Broad-Daylight-2025.pdf

11.) Jakkaru: Remote Firmware Injection in Popular Solar Inverters - Jakkaru Blog

12.) Loom, see i.a page 18: https://loomstrategy.org/wp-content/uploads/2026/04/Report_April_2026.pdf

Forthcoming: European Commission risk assessment scheduled to be conducted by mid-2026.

Note: The very recent decision of the European Commission to no longer provide any EU funding to new energy projects that include inverters connected to entities from China, Russia, Iran and North Korea gives a clear indication of the preliminary results of the upcoming official risk assessment.

European Solar Manufacturing Council AISBL
2 rue de Praetere | 1000 Brussels – Belgium

European Solar Manufacturing Council (ESMC) represents more than 60 companies across the European solar PV manufacturing value chain, including modules, cells, wafers, polysilicon, inverters, materials, equipment and energy storage.

Contact:

Christoph Podewils, Secretary General
Tel: +49 177 8741 214, email: podewils@esmc.solar

Jens Holm, Policy Director
Tel: +46 708 250 889, email: holm@esmc.solar