SolarPower Europe

Position on the adopted act to modernise the Directive on Security of Network and Information Systems

Solar Power Europe's key recommendations for the measures targeted for operators and technology vendors of distributed renewable energy assets:

- Provide detailed guidance at EU level about the type and size of relevant entities and assets targeted by the different cybersecurity risk management measures for operators of distributed renewable energy assets and for technology vendors of renewable energy asset equipment.
- Apply international and harmonised standards considering the principles of ISO27001 and IEC62443 standards to support the implementation of an actionable cybersecurity risk mitigation strategy.

SolarPower Europe's position on the adopted act on the "Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union" aiming to modernise the Directive (EU) 2016/1148 on Security of Network and Information Systems (NIS Directive).

SolarPower Europe welcomes the initiative to update the NIS Directive to address evolving security needs, and the opportunity to provide feedback to the proposal. We want to raise your attention to the following points about the scope and the measures targeted to operators and technology vendors of distributed renewable energy assets:

1. Provide detailed guidance at EU level about the type and size of relevant entities and assets targeted by the different suggested cybersecurity risk management measures.

Annex I defines the essential and important entities of the energy and electricity sectors. The scope of applicability of the cybersecurity risk management measures suggested in Article 18, is vague and needs further clarification in the body of the revised Directive or its Annexes. For this reason, it is crucial to provide detailed guidance at the EU level about the type of relevant entities and assets targeted by the suggested measures:

• **For operators of distributed renewable energy assets** (producers, suppliers, or market participants), the Directive should propose a classification of the types of targeted entities depending on the assets they operate. Relevant stakeholders should define the thresholds of the classification through a formalised process at EU level. The upcoming Network Code for Cybersecurity and the group of stakeholders involved in its development could analyse and recommend such thresholds. Obligations for cybersecurity risk management measures should be attributed to each segment based on proportionality criteria considering the levels of risk and impact of possible events per type of asset and asset fleet. Thresholds should be primarily defined addressing the assets' installed generation capacity and the total generation capacity of the fleet of assets operated by each concerned entity. This is important to ensure that assets belonging to the same type (and thus facing similar risks but operated by entities of different sizes) are subject to similar obligations (and that no competitive advantage is created for certain sizes of entities).

• **For technology vendors of renewable energy asset equipment**, a similar classification system should be created considering products with different security levels integrated by design. Relevant stakeholders should define the thresholds for equipment, assets, and entities through a formalised process at EU level. It is crucial that thresholds are harmonised across Europe to ensure the application of the single EU market concept.

Cybersecurity risk management measures should be designed with the direct involvement and collaboration of all relevant stakeholders, including both IT and OT processes and equipment. This approach will ensure a more holistic risk assessment and provide an actionable

risk mitigation strategy for distributed renewable energy assets.

2. Apply international and harmonised standards to support the implementation of an actionable cybersecurity risk mitigation strategy.

The Directive should recommend the concerned entities using standards considering the principles of ISO27001 standard or equivalent. This certification must be expanded to ensure that there is a process in place governing how cybersecurity can be guaranteed dynamically; for instance, clarifying how previously unknown vulnerabilities are treated. Renewable asset owners and technology manufacturers should have the option to choose whether they apply ISO27001 or an equivalent standard. In Table 1 we provide the relevant standards and their coverage of the recommended requirements. The IEC62443 standard covers 100% of the requirements of the ISO27001 standard. We also recommend the IEC62443 standard for industrial cybersecurity control applied to solar and wind generation assets, to cover the principal functionalities and requirements in a holistic manner.

IEC 62443 Coverage			Other Standards and Requirements Mappings
Met	Unmet	Requirements	
100%	0%	141	ISO 27001
97%	3%	108	NIST-CSF
98%	2%	171	CIS CSC-20
86%	14%	246	NERC-CIP (Americas)
80%	20%	30	NIS Directive (Europe)
90%	10%	61	JEAG 1111-2019 (Japan)

Table 1: IEC 62443 coverage of the requirements in major international standards used for OT & IT security of distributed renewable energy assets.