WindEurope's recommendations for 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 at modernising the Directive (EU) 2016/1148 on Security of Network and Information Systems (NIS Directive)

WindEurope welcomes the initiative to update the NIS Directive to address evolving security needs, and the opportunity to review and provide feedback to the European Commission's current proposal. We want to raise your attention to the following points about the scope and the measures targeted for operators and technology vendors of distributed renewable energy assets:

Detailed guidance at EU level about the type and size of relevant entities and assets targeted by the different suggested obligations.

Annex I defines which are the essential and important entities of the energy and electricity sectors. However, the scope of applicability of measures suggested in Article 18 is vague and needs further clarification in the body of the revised NIS Directive or its Annexes; there should be detailed guidance at the EU level about the type of relevant entities and assets targeted by the suggested obligations:

- **For operators of distributed renewable energy assets** (producers, suppliers, or market participants), the Directive should propose a classification of the types of targeted entities in function of the assets they operate. The thresholds for defining these types should be decided through a formalised process with all relevant stakeholders' involvement. The upcoming Network Code for Cybersecurity and the group of stakeholders involved in its development could analyse and recommend such thresholds. Obligations for risk management measures should be attributed to each type 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 (in case interaction and impact among assets of the same operator needs to be considered). Considering these criteria is very 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 grading should be created considering products with different security levels integrated by design. The respective thresholds for equipment, assets and entities should be defined through a formalised process at the EU level involving all relevant stakeholders. They should be harmonised across Europe to ensure the application of the single EU market concept.

- **Further to thresholds, suggested risk management measures** should also 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.

Application of international and harmonised standards to support the implementation of an actionable risk mitigation strategy.

The Directive should recommend using the ISO27001 standard or equivalent to be applied by the concerned entities. Renewable asset owners and technology manufacturers should have the option to

choose whether they will apply ISO27001 or an equivalent standard. In the Annex, we provide a table mapping the different relevant standards and coverage of recommended requirements (Table 1). When it comes to industrial control cybersecurity applied to wind and solar generation assets, the IEC62443 standard is the recommended one for covering the principal functionalities and requirements in a holistic manner. Further to these recommendations supporting the use of international standards, the EC could help ENISA to develop an EU minimum applicable standard that could be used by all concerned entities without requiring compliance with this one or the previously mentioned international standards.

IEC 62443 Coverage			Other Standards &
Met	Un Met	Reqs	Requirements Mappings
97%	3%	108	NIST-CSF
98%	2%	171	CIS CSC-20
100%	0%	141	ISO 27001
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 requirements in major international standards used for OT and IT security of distributed renewable energy assets