Union Française de l'Électricité

March 2021

Position Paper

UFE's position on the European Commission's proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148

The French electricity industry (UFE) welcomes the European Commission's proposal for a new Directive on network and information system (known as the NIS 2 Directive), as further harmonisation and reinforcement of cybersecurity across sectors and Member States are needed. To ensure effective implementation of the Directive, UFE would like to highlight some key elements:

1. A high level of cybersecurity across the EU can only be achieved through a systemic approach

A systemic approach to cybersecurity is needed to ensure a high level of protection in the EU. In our increasingly interconnected economy, cybersecurity can no longer be guaranteed by protecting only specific infrastructures, but rather by ensuring the protection of a service delivery from end to end. Therefore, **UFE supports the extension of the scope of the Directive to more sectors and subsectors**.

- **UFE welcomes the deletion of the former categories** of "operators of essential services" and "digital service providers". The introduction of a new distinction between essential entities and important entities, with **identical risk management and reporting obligations** applying to both categories, is a significant improvement.
- The **inclusion of new sub-sectors of the power system** in the scope of the Directive (namely electricity producers, NEMOs and market participants providing aggregation, demand response or energy storage services) will help ensure a **higher level of cybersecurity and cyber-resilience of the power system as a whole**.

Union Française de l'Électricité

2. The size-cap rule does not address properly the risks faced by the power sector

Given the increasing interdependency of the various components and actors of the EU interconnected power system, the size-cap rule does not seem appropriate to address the cybersecurity risks faced by the power sector from end to end. Nevertheless, the same high requirements cannot apply to all entities regardless of their size and resources.

According to the European Commission's proposal, **micro and small enterprises** (i.e. which employ less than 50 employees and which turnover does not exceed 10M€) are not included in the scope of the Directive. Applied to the power sector, this means that **a significant number of actors will not be subject to any cybersecurity requirements.** For instance, electricity producers with an installed capacity of up to 10MW[1] would not be subject to the protective measures provided by the Directive.

However, **a coordinated cyberattack** (either simultaneously or by domino effect) **on several small entities** of the electricity system (e.g. small producers, operators of EV charging infrastructures) could put the whole European power system under great stress and even endanger it, by causing significant imbalances and hampering the management of the system.

That said, UFE stresses that **the right balance needs to be found regarding requirements for micro and small enterprises** from the power sector.

- As the number of small actors in the electricity sector is expected to increase significantly in the coming years, **it is of utmost importance to ensure that minimum cybersecurity risk management and reporting obligations apply to them. These requirements must be proportional to their capabilities and the cost of implementation relative to their size.**

3. Financial incentives are needed to accompany essential entities of the power sector in the implementation of the NIS 2 Directive

Given the important investments foreseen to comply with the requirements set out in the NIS 2 Directive, **financial mechanisms and incentives should be explored at both EU and national levels** to help the increasing number of essential entities in the implementation. It appears of utmost importance to accompany a sector at the heart of the transition to a climate-neutral economy in its digital transition.

4. Essential entities and their targeted network and information systems must be clearly defined

There is some confusion as regards what can be considered as an essential entity in the energy sector: the list set out in Annex I refers either to specific actors (e.g. producers) or general activities (e.g. district heating and cooling).

[1] This is an indicative threshold, some producers with a higher installed capacity may not be subject to the provisions of the Directive either.

- It is necessary to **make a clear reference to legal entities** (i.e. natural or legal person) in Annex I, as provided by Article 4(24).

We also see a need to **clarify the scope of the cybersecurity obligations of essential and important entities**, to avoid any misinterpretation that would lead to a broadening of the scope of the Directive to all components of the IT systems of targeted companies, even when not necessary. This could lead to **unnecessary costs and administrative burden**. A flexible implementation of the NIS 2 Directive will be needed to ensure its requirements are materialised in a manner commensurate with the risk identified by the targeted entities.

- Article 18(1) should be modified as follow to specify that cybersecurity risk management measures **only apply to important and essential services**: "Member States shall ensure that essential and important entities shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which those entities use in the provision of ***their important and essential*** services."

5. A mutual exchange of information between national authorities and essential entities is needed

The reporting requirements set out in the Directive are useful mechanisms which will help guarantee a high level of cybersecurity in the EU.

Nonetheless, **the Directive should guarantee a mutual exchange of information** between national CSIRTs or national authorities on one hand and essential entities on the other hand, **to increase the level of awareness of the relevant actors in case of cybersecurity risk**.

- This could be done by ensuring **that internal CSIRTs of essential entities are notified without delay of any major incident occurring in their sector**.

6. Non-EU service providers should be subject to minimum cybersecurity risk management requirements

Essential entities located in third countries and providing services in the EU should not be exempted from guaranteeing a certain level of cybersecurity.

- The possibility to **establish cybersecurity standards that would apply to non-EU essential entities** should therefore be further explored.