April 2018

Position Paper

Cybersecurity Act

The French Union of Electricity welcomes the release of the « Cybersecurity Package » by the European Commission, which shows the Commission's focus on cybersecurity matters. In an increasingly connected world, it is our common responsibility to fight against cyber-attacks and protect strategic infrastructures.

The French Union of Electricity supports the European Commission's desire to enhance the means allocated to cybersecurity in the European Union. The legal frameworks and technical solutions implemented must help Member States in their progress to cyber-secure themselves.
However the Commission's proposal does not give Member States the necessary instruments to actually strengthen Members States' cybersecurity level.

As the regulation proposal includes plans to reinforce the ENISA, the French Union of Electricity would like to stress that reinforcing the ENISA should not lead to a decrease in the cybersecurity performance already reached in some Member-States thanks to their own national cybersecurity Agencies.

For several years, French energy companies have developed a trust-based relationship with ANSSI (the National Agency for Security of Information Systems), based on a deep understanding of essential services operators, their industrial processes and the existing threats. ANSSI has given itself the means and expertise to enable it to reach and demand the highest levels of cybersecurity. The creation of such an agency involved certain essential prerequisites: trust among the parties built over time, a high level of expertise and means to take action.

The proposal to implement a European certification scheme, which would replace existing national ones, also poses a risk for Europeans industries. As energy companies rely on connected objects they work with, trust in the quality and security of these objects is very much necessary. This trust can be built through certification schemes with strict requirements and that require devices to undergo thorough testing. The creation of a European certification scheme should in no way undermine existing security measures, and should instead be based on existing and proven high-level security schemes. It is essential that national agencies do not lose their operational capacity. Indeed, national certification should remain valid. Finally, European certification, depending on the sensitiveness of information system, should only provide minimum mandatory requirements.

In addition, further clarity with regards to the scope of the regulation seems necessary to ensure maximum security, insomuch as the certification scheme applies to services and products, but not necessarily to all the actors involved in such services and products. **Protection should be ensured from a systemic perspective, so as to certify the entire value chain as well as cover the whole life cycle of ICT products and services in their processes and systems**, from their design to the dismantling.

ENISA’s enhanced role should aim at helping less advanced Member State to reach a common European level of security, while at the same time giving the other Member States the opportunity to develop even higher standards, in order to push for a single European cybersecurity standard of excellence. The Agency must ensure harmonisation and coherence of European provisions to allow a gradual increase towards more advanced cybersecurity levels.