

18th March 2021

Feedback to the proposed revision of the NIS Directive



CURRENT

Enabling Network Technology
throughout Europe



currENT is an industry association that represents the voice of Europe’s innovative grid technology companies. Our vision is a European power network that is the recognised world leader in enabling decarbonisation through the efficient use of modern grid technology and digitalisation.

currENT believes renewable generation, coupled with electrification, is the ‘first order’ solution for the economic decarbonisation of Europe. Power networks – both transmission and distribution – must become even stronger enablers and accelerators of the energy transition.

Digitalisation is key to making the energy transition happen. The Commission just last week emphasized the transformative potential of the present Digital Decade as critical in transitioning to a climate neutral, circular and resilient economy.¹ The transition to renewable energy sources means that new generation will come into the grid at more numerous and widely distributed locations than ever before. It will be augmented by a range of new devices, sensors and software which will open up opportunities to use the grid in new ways, ranging from using big data and machine learning to enhance system optimization to new ways of empowering consumers.

Such changes create opportunities to move the energy transition from ‘can do’ to ‘will do.’ **currENT**’s members offer solutions that climate-proof existing power networks and add innovative elements to the new ones that are yet to be built. Existing power networks can be optimised and reinforced through these solutions, and additional networks can start off with the latest state-of-the-art technology. Our solutions enable power networks to deliver the energy transition at least cost, in a secure, sustainable and socially responsible manner.

currENT welcomes the Commission’s initiative to review the existing Network and Information Security (NIS) Directive. Safe and reliable electric service has long been understood to be a fundamental underpinning of modern society. Customers and regulators alike have a high degree of expectation that utilities will “keep the lights on,” and utilities have long taken seriously the need to ensure operational security. In order to reap the benefits of digitalisation, it is therefore essential to ensure that cybersecurity risk in networks is managed effectively and does not become a roadblock to digital energy.

As a proponent of technological grid innovation and an advocate of collaborative engagement, **currENT** has endeavoured to help further discussion of these issues in the energy context. Most recently, **currENT** organized a webinar to bring together a range of perspectives on electricity grid digitalisation and cybersecurity in Europe,² and **currENT** looks forward to further engagement with the stakeholder community in working through issues relating to the cybersecurity network codes and ECI Directive.

While the original NIS Directive was an important step in providing EU-wide legislation on cybersecurity, comments which were submitted in the Open Public Consultation (OPC) make clear there is significant

¹ European Commission, ‘Europe’s Digital Decade: Commission sets the course towards a digitally empowered Europe by 2030’ (2021), https://ec.europa.eu/commission/presscorner/detail/en/IP_21_983.

² **currENT**, ‘Accelerating the Energy Transition: Cybersecurity, Digitalisation and the Electricity Grid in Europe’ (2021), <https://www.currentheurope.eu/conclusions-cybersecurity-digitalisation-and-the-electricity-grid-in-europe/>.



consensus that additional refinements needed to be made. **currENT** welcomes the new proposal's efforts to provide for better and more consistent cybersecurity resilience, joint situational awareness, and incident reporting and response across Member States and industry sectors. Like the digital economy, the electric grid is by its nature a cross-border enterprise which is driven by forces that transcend traditional national boundaries. The energy transition will most efficiently meet the needs of all Europeans when we can source power from where it can be produced most cleanly and cost-effectively to where it can be consumed by customers who need it.

currENT therefore supports approaches which seek to streamline and harmonize cross-border security requirements, and which attempt to avoid creating excessive regional differences or creating silo-type approaches to incident response and data sharing. In reviewing the OPC,³ we note very strong consensus on aligning cybersecurity rules at the EU level, and significant concerns where approaches fail to be harmonized and/or result in fragmentation that may increase transaction costs and/or prevent level playing fields between Member States. Making a distinction to prefer measures which are outcome-focused as opposed to more prescriptive requirements seems sensible.

Finally, **currENT** notes concerns about applying costly rules to smaller enterprises. Although there appears to be some consensus that cybersecurity improvements under the original NIS Directive has been achieved at reasonable cost, **currENT** appreciates the Commission's continuing sensitivity going forward as to their impacts on smaller entities.

³ European Commission, 'OPEN PUBLIC CONSULTATION ON THE DIRECTIVE ON SECURITY OF NETWORK AND INFORMATION SYSTEMS ('NIS DIRECTIVE')' (2020), <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Revision-of-the-NIS-Directive/public-consultation>.