



The European Association of the Electricity
Transmission and Distribution Equipment
and Services Industry

T&D Europe welcomes the adoption of the Cybersecurity Network Codes

26 March 2024

T&D Europe, the European Association of the Electricity Transmission and Distribution Equipment and Services Industry, **would like to welcome and use this opportunity to raise our concerns on the Cybersecurity Network Codes.**

Key points:

1. T&D Europe welcomes the adoption by EU Commission of the Network Code for Cybersecurity.
2. Development of supply chain security measurements and procurement recommendations should involve the collaboration of all interested parties.
3. T&D Europe requests that EN ISO/IEC 27001, EN IEC 62443 and EN IEC 62351 framework references are acknowledged as industry benchmarks.

Network Codes for Cybersecurity

T&D Europe welcomes the adoption of the Network Code for Cybersecurity for cross border flows. This follows a long-term development programme by the European Commission, ACER, ENTSO-E and EU-DSO and in which T&D Europe experts actively participated.

T&D Europe believes that the cybersecurity network code can make a positive impact on the electricity sector by bringing together all the authorities and actors participating in the market.

The Network Code arrives in a particularly sensitive moment when several EU cybersecurity legal initiatives are being revised or developed, such as the recent adoption of NIS2, that brings the electrical equipment industry into scope, the Radio Equipment Directive-Delegated Act and the Cyber Resilience Act. As a result, there are several elements of the cyber resilience legal framework in development simultaneously which will increase the challenges for technology providers.

T&D Europe highlights the large number of new operational documents that will act as mandatory references for the sector that will be developed and executed under the network codes by ENTSO-E and EU DSO as described in Article 6. It is T&D Europe's view that it is important for those tasks to be executed in cooperation with sector technology and solution providers and therefore calls attention to **Article 10 – Stakeholder involvement** as a major success factor in achieving the ambitions described in the subsequent articles. T&D Europe specifically states that supply chain measurements and procurement recommendations will greatly benefit from the collaboration of all interested parties.

T&D Europe also points out that its members have been heavily investing in the security and interoperability of solutions and products for the past decade and have adopted international and European standards such as **EN ISO/IEC 27001, EN IEC 62443 and EN IEC 62351 frameworks** to name the most relevant ones for our cybersecurity posture, manufacturing lines, project deployment and the cybersecurity of our products. This work has been aimed towards ever higher level of security posture maturity and a long-term commitment to our partners and customers.

We in T&D Europe expect that those standard references are acknowledged as industry benchmarks and that they are referenced and used in the Cybersecurity Network Code deployment.