Brussels, 12 May 2026

BDEW Bundesverband
der Energie- und
Wasserwirtschaft e.V.
(German Association of Energy and
Water Industries)
BDEW Representation at the EU

Avenue de Cortenbergh 52
1000 Brussels
Belgium

www.bdew.de

Position Paper

Cybersecurity Act (CSA) 2

Version: final

Contents

1 Key messages from BDEW

The German Association of Energy and Water Industries (BDEW) supports the revision of the Cybersecurity Act (CSA) as part of the legislative proposal for CSA 2 of 20 January 2026. The European Commission aims to strengthen cybersecurity capabilities and resilience, as well as preventing the fragmentation of the EU's digital single market.

A coherent, risk-based and practical European framework is crucial. It must strengthen resilience, avoid new operational risks and unnecessary bureaucracy, and take into account the operational realities of critical infrastructure. It is essential that CSA 2 actually increases resilience without creating new burdens through additional complexity or impractical requirements.

2 Strengthen ENISA and standardise reporting channels

Position: In view of the increased cyber threat landscape, Europe needs an effective agency that publishes cross-border situational assessments, identifies risks at an early stage and quickly passes on relevant information to affected organisations.

BDEW calls for:

- Preventing additional administrative burdens or parallel structures in reporting channels.
- Ensuring secure transmission channels and reliable data storage.
- Deriving concrete operational value for businesses from reports and situation assessments.

Context: Robust situational assessments with actionable information for operators (e.g. *Indicators of Compromise* or recommendations for action), clear thresholds and well functioning feedback channels are crucial for companies in the energy and water sectors. In this regard, a uniform European reporting approach can strengthen resilience and reduce bureaucracy, provided the flow of information is designed to be bidirectional.

3 Design ICT supply chain security risk-based and resilience-oriented

Position: BDEW supports the objective of enhancing the security of European ICT supply chains. In the energy and water sectors, the integrity, availability and controllability of components and systems used are of paramount importance. However, the "ICT Supply Chain

Framework" under CSA 2 entails, in some cases, far-reaching changes for the procurement of components in the energy sector, as part of the critical NIS 2 sectors, primarily due to the shift from a cost-driven to a security and geopolitics-driven procurement. Furthermore, there are already far-reaching regulations governing the use of critical components under national legislation, particularly in the German Energy Industry Act („Energiewirtschaftsgesetz“, EnWG) in conjunction with the German Act on the Federal Office for Information Security („Gesetz über das Bundesamt für Sicherheit in der Informationstechnik“, BSIG). It is therefore essential to avoid duplication here.

BDEW calls for:

- Regulatory requirements to be designed in such a way that they strengthen resilience and do not create new risks through abrupt replacement obligations, overly complex procedures or unrealistic deadlines.
- If a ban is imposed on technology that has already been installed and which, given its life cycle, does not yet need to be replaced, compensation must be provided for stranded investments.
- Potential bans also have a significant impact on negotiating positions vis-à-vis other suppliers. If the legislator, in the interests of public security, bans certain components or suppliers, it must simultaneously support opportunities for the domestic economy to manufacture components with comparable performance (and at comparable prices) within the EU.
- Particularly in long-cycle OT (operational technology) infrastructures, sufficient predictability, realistic transition periods and operational continuity must be ensured. Retroactive requirements undermine planning certainty.
- Risks must be considered in a differentiated manner and not narrowed down solely to the manufacturer level. Instead, manufacturer, product and system risks must each be assessed independently. In doing so, interactions during integration, technical manageability during operation, and the impact on the stability and security of existing infrastructures must also be taken into account. The effects of data flows and cloud solutions should also be considered.
- Resilience requirements should be designed in such a way that realistic transformation pathways and actual feasibility in complex existing environments are taken into account.
- Ensuring coherence with other sectoral regulations with similar objectives, in particular the Industrial Accelerator Act (IAA) and the proposed amendments to the Net Zero Industry Act (NZIA) contained therein, the Critical Raw Materials Act (CRMA), the AI Act (particularly regarding ‘Toxic AI’), and the national requirements for critical

components under the abovementioned German Energy Industry Act (EnWG) in conjunction with the German BSIG.

Context: Particularly in complex migration environments, short-term regulatory interventions can trigger significant operational risks. Regulation should therefore take security of supply and technical feasibility into account from the outset.

4 Accelerate certification frameworks and make them practical

Position: The European certification framework should make security requirements transparent, strengthen trust and fulfil regulatory compliance obligations more efficiently. However, this requires that (security) certification be practical, cost-effective and reliable. From the perspective of companies, it is crucial that certification requirements are designed to be compatible with existing operational and maintenance processes. A lack of alignment with established update and maintenance cycles leads to significant implementation risks, particularly for legacy systems and in markets with limited supplier diversity. Certification requirements should therefore take greater account of the actual technical, economic and market structural conditions.

BDEW calls for:

- Certification schemes to be made more transparent and more closely aligned with international standards.
- Certificates to be recognised across the EU as reliable proof in order to avoid duplicate testing and prevent market foreclosure caused by national security requirements and certification procedures.
- Costs and administrative burdens to be limited to a cost-effective and proportionate level.
- Recertification and update processes to be designed innovation-oriented.
- Planned changes and continuous improvements to certification requirements to be designed with sufficient predictability and appropriate transition periods, so that they can be integrated into existing operational and update processes, as every change entails effort and adaptation within the security model, and aligned with major recertification cycles.

Context: Experience from the smart meter sector in Germany shows that lengthy and complex certification processes can significantly slow down innovation and implementation of technology. At the same time, certification requirements should remain sufficiently risk-oriented and practical; overly detailed procedural requirements restrict operational flexibility and increase

the burden. A more uniform European framework should also strengthen the mutual recognition of security certifications, thereby simplifying certification procedures across national borders.

5 Better coordinate existing EU cyber regulations

Position: The CSA 2 should be closely aligned with the NIS2 Directive, the DORA Regulation (Digital Operational Resilience Act), the Cyber Resilience Act (CRA) and other sector-specific requirements. A coherent and consistent legal framework is of central importance for companies in the energy and water sectors.

The BDEW calls for:

- European cyber requirements to be consistently harmonised, and for proven national and sectoral implementation approaches to be changed only if it results in clear added value for cybersecurity, resilience and legal clarity.
- Double regulation and multiple reporting requirements to be avoided.
- Appropriately taking into account, standardising and harmonising sector-specific characteristics and the reality of multi-utility companies.
- Special provisions or suitable opening clauses that are practicable at European level for multi-sector companies.
- Avoid additional national tightening of regulations where possible, or at least secure national recognition through uniform standard requirements.
- Promote risk-based and sector-specific requirements that can be integrated, taking due account of existing protected assets and the operational realities of critical infrastructure.

Particular need for action regarding multi-sector companies

The planned amendment to the NIS2 provisions in the field of electricity generation could have significant consequences for companies that generate energy only to a minor extent, but whose main activity lies in another sector. Specifically, in its legislative proposal for a directive amending the NIS2 Directive and aligning it with the CSA 2 (COM (2026) 13 final), the European Commission proposes in Annex 1 that generators with a generation capacity of 1 MW or less should be excluded from the scope of NIS2. However, this contradicts existing exemptions under the German implementation of the NIS2 Directive (see Section 28(3) and (4) of the BSIG). If European special provisions are narrowed, there is a risk of new legal uncertainties and additional regulatory burdens. Proven national definitions for ancillary

activities and activities of negligible significance should therefore not be lost without any clear added value in terms of security.

Context: In regulated infrastructure sectors, differentiated verification, testing and security structures already exist, which are adapted to the respective operational realities. New European requirements should build on these structures and design them to be compatible, rather than creating additional parallel regimes or unnecessary conversion costs.

6 Possible sector-specific full harmonisation through EU implementing acts

Position: The proposed new Article 5 of NIS2, in conjunction with Article 21(5), gives the EU Commission the power to harmonise technical, methodological and sector-specific cybersecurity requirements across the EU by means of implementing acts in the future. This is of considerable importance for the energy and water sectors.

The BDEW calls for:

- Any sector-specific implementing acts to be adopted only with the close involvement of the sectors concerned.
- Practical transition periods and the consideration of existing sector-specific characteristics, in particular long-cycle OT infrastructures and high resilience requirements, to be ensured.
- In the event of full harmonisation, to take into account conversion costs, migration risks and interactions with existing national regulations at an early stage, and to allow new European requirements to intervene in existing security regimes only where there is demonstrable added value.

Context: The proposal does not yet contain any sector-specific requirements for the energy sector, but expressly opens up the possibility for the Commission to adopt such requirements in the future. Given the cross-border relevance of the energy sector, a subsequent EU-wide specification of the NIS2 risk management measures cannot be ruled out.

7 Conclusion

CSA 2 offers the opportunity to make the European cyber framework more effective, coherent and practical. From BDEW's perspective, it is essential to strengthen the resilience of critical infrastructure in a targeted manner without creating new operational risks or unnecessary layers of bureaucracy. Key factors here are clear added value for the companies concerned, risk-based regulation and a framework that takes appropriate account of technical realities, security of supply and operational feasibility.