FEDIL

Positionen

POSITION ON THE REVISED EU CYBERSECURITY ACT (CSA2)

Zusammenfassung / Inhalte

EXECUTIVE SUMMARY

- Strengthening cyber resilience, reinforcing EU level coordination through ENISA and improving coherence across the EU cybersecurity acquis (notably NIS2, the Cyber Resilience Act and DORA) are legitimate and timely objectives.
- At the same time, cybersecurity regulation must remain fully compatible with Europe's competitiveness agenda and the proper functioning of the Single Market.
- Cyber resilience, technological sovereignty and economic competitiveness are mutually reinforcing objectives and must be pursued together through a proportionate, risk based and technology neutral framework.
- Cybersecurity is best achieved through diversification, competition and redundancy in supply chains, rather than through broad supplier restrictions that reduce supplier diversity, increase costs and undermine investment predictability.
- The CSA2 framework must remain proportionate and risk based, technology neutral, predictable and legally certain.
- CSA2 should genuinely simplify and align existing obligations across the EU cybersecurity acquis, avoiding additional layers of regulatory complexity that could divert resources away from effective risk

reduction.

GOVERNANCE AND ENISA'S ROLE

- A stronger and better resourced ENISA acting as a centre of coordination, expertise and support at EU level, notably through enhanced situational awareness, capacity building and support to Member States is welcomed.
- This reinforcement must remain clearly bounded and technocratic in nature, preserving the institutional balance and national competences and avoiding mandate inflation or excessive prescriptiveness.
- ENISA should not evolve into a de facto regulator or standard setter; formal standardisation must remain the responsibility of European Standardisation Organisations (ESOs), with ENISA focusing on coordination and facilitation.
- Robust governance, accountability, confidentiality and data handling safeguards are essential to maintain trust between authorities and industry.

EUROPEAN CYBERSECURITY CERTIFICATION FRAMEWORK

- Cybersecurity certification is welcomed as a presumption of conformity across EU cybersecurity legislation and as a practical compliance tool for businesses.
- Certification must remain voluntary, risk based and interoperable with NIS2, the Cyber Resilience Act, DORA and sector specific frameworks, and must not become a de facto market access requirement.
- CSA2 should prevent the proliferation of overlapping schemes, ensure realistic timelines for scheme development and maintain meaningful, structured and continuous industry involvement throughout scheme development and implementation.
- Certification should function as a genuine compliance enabler, reducing duplication and administrative burden rather than adding new regulatory layers.

ICT SUPPLY CHAIN SECURITY AND HIGH RISK SUPPLIERS

- While addressing non technical risks and geopolitical dependencies is legitimate, the proposed framework raises serious concerns regarding proportionality, legal certainty and market impact.
- Broad supplier restrictions risk reducing competition, forcing reliance on a limited number of suppliers, increasing costs, creating capacity bottlenecks and delaying network upgrades, without necessarily delivering proportionate security gains.
- Any new restrictive measures must remain evidence based, transparent and risk driven, be subject to robust due process safeguards and thorough impact assessments.
- Exclusion of suppliers should remain a measure of last resort, and priority should be given to targeted mitigation measures.
- Legal certainty is further undermined by insufficient clarity regarding the scope of key ICT assets and by asymmetric transition periods across network types.
- Clear and exhaustive definitions of key ICT assets must be set directly in the regulation, and transition periods must be predictable, technology neutral and applicable to all network types reflecting operational and investment realities.

ECONOMIC IMPACT AND COMPENSATION

- The broader economic impact of large scale supplier changes appears to have been underestimated. Preliminary indications from independent European studies point to significantly higher costs than envisaged in the Commission's impact assessment.
- The absence of a financial compensation mechanism is a major shortcoming, given the substantial investments already made by operators in equipment that may need to be phased out for politically driven reasons.
- Appropriate compensation mechanisms are necessary to preserve investment confidence, ensure fair treatment and avoid undermining the economic viability of infrastructure operators.

FEDIL CALLS ON EU CO LEGISLATORS TO:

- ensure a proportionate, legally certain and risk based CSA2 framework,
- preserve competition, diversification and investment predictability in ICT supply chains,
- maintain a balanced governance model with a clearly defined and bounded role for ENISA,
- make cybersecurity certification a practical, voluntary and effective compliance enabler,
- substantially recalibrate Title IV, including scope clarity and predictable transition periods,
- reassess the economic impact of supplier changes and introduce appropriate compensation mechanisms,
- ensure proportionate, fair and predictable enforcement mechanisms.

READ THE FULL POSITION