EuroISPA Contribution to the proposal on CSA 2.0. and the Directive on Simplification Measures and Alignment with the Cybersecurity Act

May 2026

EuroISPA welcomes the European Commission's proposals for a revised Cybersecurity Act (CSA 2.0) and the accompanying Directive on simplification measures and alignment with the Cybersecurity Act (NIS2 Simplification Directive) as important steps towards strengthening the European cybersecurity framework. We support the objectives of reinforcing ENISA's mandate, improving coordination, and enhancing the effectiveness of the EU's cybersecurity certification system.

At the same time, further efforts are needed to ensure genuine simplification and harmonisation across the regulatory landscape. In particular, the introduction of non-technical requirements risks adding complexity and undermining the technical integrity and neutrality of existing frameworks. Certification schemes under CSA 2.0 should therefore remain strictly technical, while international standards, such as ISO frameworks, should be consistently promoted to ensure interoperability and clarity.

EuroISPA also supports stronger stakeholder engagement and the integration of technical expertise within an enhanced ENISA mandate.

Regarding the NIS2 framework, while we welcome targeted amendments, including the introduction of a new regime for mid-cap enterprises, additional progress is needed to reduce overlapping reporting obligations and to ensure the effective application of the principle of maximum harmonisation across Member States. This should include, in particular, the adoption of a 'single audit' approach.

Building on these considerations, EuroISPA puts forward the following recommendations to support co-legislators in developing a secure, resilient, non-bureaucratic and globally competitive European cybersecurity ecosystem, while avoiding unnecessary regulatory burdens.

EuroISPA
Rue de la Loi 38, 1000 Brussels
secretariat@euroispa.org
EU Transparency Register: 54437813115-56

1. **Strengthen ENISA's Mandate and Coordination Role**

ENISA should play a central role in identifying regulatory divergences across Member States, providing technical guidance, and ensuring coherence within the cybersecurity single market. In this context, ENISA should:

- conduct security impact assessments;
- provide clear guidance on applicable standards, including promoting international frameworks such as ISO/IEC 27001;
- strengthen its role in international standardisation to ensure EU interests are effectively represented.

2. **Preserving Technical Rigor and Structured Industry Participation in the European Cybersecurity Certification Framework**

We welcome the revision of the several structural improvements to the ECCF that provide much-needed predictability, agility, and international alignment. Nevertheless, we believe that certification schemes developed under the CSA 2.0. should remain exclusively technical in nature and any introduction of non-technical risks should be addressed under the Supply Chain Framework. Preserving this separation is essential to maintain the framework's technical integrity

We strongly support the Commission's stated ambition to enhance transparency and stakeholder engagement throughout the planning, development, adoption, and maintenance stages of certification schemes. Nevertheless, the new European Cybersecurity Certification Assembly's mandate is to ambiguous and only allows for once-a-year discussions on strategic priorities. Shifting from a permanent industry stakeholder expert group to an annual, large-scale assembly greatly limits the industry's capacity to provide ongoing, regular, detailed, and structured input on the design of new schemes and the governance of the framework. This change risks further diluting already limited industry engagement, including the risk of limited legal predictability and certainty, which goes against the overall promised simplification and regulatory effectiveness objective and should be carefully reconsidered.

3. **Safeguarding Risk-Based Assessment in the Cyber Posture approach**

The introduction of the "cyber posture" approach introduced in Title III of the CSA 2.0. shifts the focus from specific products and services to the assessment of entire entities, including their virtual and physical infrastructure. While streamlining compliance is a legitimate aim, the approach is insufficiently defined and overly broad, as evaluating an organization's overall security standing risks introducing subjective or non-technical considerations into an otherwise objective, evidence-based certification process. The overall legal uncertainty is given also by unclear rule whether such assessment will be done ex ante or ex post. We strongly caution against any move to make this posture mandatory under the NIS2 regime. Any expense needed to handle and understand complex obligations is an expense stolen to real cybersecurity operations (investments in devices and investments in technical employees).

4. Strengthening Objective, Risk-Based Approaches in the EU ICT Supply Chain Security

EuroISPA believes that non-technical considerations introduced under Title IV, such as sovereignty-based criteria, should remain clearly separated from cybersecurity certification schemes to preserve their technical neutrality and legitimacy. Introducing such elements risks fragmenting the internal market, creating legal uncertainty, and undermining competitiveness.

Moreover, the use of Article 114 TFEU as a legal basis appears inconsistent where measures pursue broader geopolitical objectives rather than evidence-based cybersecurity outcomes. Member States already retain effective tools to address national security risks in ICT supply chains. An EU-level approach should therefore remain focused on objective, technical risk assessment, while respecting the principles of subsidiarity and conferral.

5. Establishing Objective, Entity-Based Criteria for High-Risk Suppliers

The current framework risks overemphasising factors such as a supplier's country of origin, without sufficiently accounting for the actual technical security and integrity of individual entities. EuroISPA therefore calls for the establishment of clear, objective and evidence-based criteria for risk designation, including transparent documentation and robust technical justification prior to any restrictive measures.

The process should also include appropriate safeguards against politicisation. In particular, designations triggered by individual Member State statements, or through emergency procedures, should remain exceptional, proportionate, and subject to subsequent full risk assessment, including a clear mapping between identified risks and the measures imposed. Impact assessments should be conducted in advance, and relevant technical and sectoral experts systematically consulted, given the wide range of sectors covered by Annex I and II of the NIS2.

A more granular, case-by-case approach is essential to ensure proportionality and legal certainty. This is particularly important in market segments where the availability of commercially viable and scalable alternatives remains limited. Removing suppliers without ensuring accessible substitutes risks distorting competition, disproportionately affecting smaller operators, and reinforcing market concentration.

Finally, cybersecurity policy should remain grounded in observable risks and technical evidence. Available evidence indicates that data exfiltration more frequently occurs through software vulnerabilities and user applications rather than hardware provenance alone. An approach that focuses narrowly on vendor origin, without addressing broader systemic vulnerabilities, risks providing a false sense of security while leaving critical attack vectors insufficiently addressed.

6. Evaluating the Impact of Mandatory ICT Asset Phase-Out

EuroISPA is concerned that the approach under Title IV may lead to the exclusion and premature replacement of ICT assets without sufficiently objective, evidence-based risk assessment. Such measures risk being disproportionate and could result in significant technical, financial, and operational disruption across the electronic communications ecosystem.

Mandating the early replacement of functioning equipment would impose substantial costs on operators, including the decommissioning of existing infrastructure, procurement of replacement technologies, and the operational burden of migration, testing, and ensuring service continuity. By way of example, internal estimates from a national ISP association indicate that, for the SME operator segment in Italy alone, these combined costs could exceed EUR 1 billion. These impacts would likely divert resources away from core cybersecurity investments and resilience-building efforts.

Beyond the direct financial burden, large-scale asset replacement risks weakening Europe's digital ecosystem by disrupting ongoing investment cycles, delaying network deployment, and placing additional strain on operators with limited financial and technical capacity. These effects would be particularly pronounced for smaller and mid-sized providers.

Such an approach would also run counter to EU environmental and sustainability objectives. Forcing the early decommissioning of operational equipment would accelerate the generation of electronic waste and shorten asset lifecycles, undermining efforts to promote resource efficiency and sustainable digital infrastructure.

In this context, preserving asset longevity where technically appropriate, combined with a pragmatic approach to diversification of supply sources, is essential to ensuring long-term resilience. Rather than mandating large-scale replacement, policy should prioritise risk mitigation, lifecycle management, and operational flexibility, allowing operators to address security concerns in a proportionate and economically sustainable manner.

7. Enable Simplification and Harmonisation Across Frameworks

Simplification of obligations across EU cybersecurity frameworks is essential. Currently, companies face multiple and overlapping reporting requirements under NIS2, the Cyber Resilience Act (CRA), the GDPR, and the Digital Operational Resilience Act (DORA), creating unnecessary administrative burden and diverting resources from effective cybersecurity measures.

While the Commission's cybersecurity package introduces welcome simplification efforts, these remain insufficient. EuroISPA calls for harmonised reporting thresholds across frameworks and the establishment of a single reporting point for cybersecurity incidents in each Member State. Harmonisation should apply not only across Member States but also across sectors and legislative instruments, ensuring consistency in scope, reporting obligations, security requirements, and oversight.

For entities operating cross-border, inconsistent national supervisory practices and duplicative security audits significantly increase compliance costs and complexity. EuroISPA therefore strongly supports the introduction of a 'single audit' principle under the NIS2 Simplification Directive, allowing compliance in one Member State to be recognised across the internal market.

Finally, the principle of maximum harmonisation must be effectively implemented. Compliance with Union-level rules should be sufficient to meet national requirements, avoiding additional or fragmented "gold-plating" by Member States.

8. **Introduction of the New Regime Mid-Cap Organisations and Removal of Small and Micro-DNS Service Providers**

We welcome the NIS2 simplification efforts, in particular the creation of a new regime for mid-cap organisations and the removal of small and micro-DNS service providers from the scope of NIS2. This regime is particularly vital because SME and mid-cap operators often invest most intensively in peripheral and less-served territories. These entities have the least bargaining leverage with global vendors and the lowest fiscal capacity to absorb the high costs of 'political' exclusions. The framework must ensure that security requirements do not lead to artificial market concentration, which would leave these essential regional providers with fewer components and higher prices.

We believe these measures help reduce the compliance burden for both subject entities and competent authorities.

9. **Exempt Internally Developed Tools Not Placed on the Market**

EuroISPA recommends introducing a clear exemption for software, firmware, and ICT components developed and used internally. Certification should only apply when such tools are placed on the market or used in critical infrastructure contexts. This approach avoids unnecessary regulatory burdens on internal tools that are not intended for broader commercial or public use.

10. **Recognise the Importance of Open-Source and Small-Scale Developers**

The CSA 2.0. should explicitly acknowledge the vital role of open-source communities, SMES, and independent developers within Europe's cybersecurity ecosystem. These actors make a significant contribution to resilience and innovation and should not be hindered by certification schemes that are overly complex or financially burdensome. In this regard, EuroISPA believes that exempting them from certification fees would be a positive step. Their work enhances Europe's technological diversity and sovereignty and should be supported through a proportionate and inclusive regulatory approach.

To conclude, the CSA 2.0 represents a key opportunity to strengthen the EU's cybersecurity framework while supporting a competitive and resilient digital ecosystem. Achieving these objectives requires a balanced and evidence-based approach that preserves the technical nature of certification schemes, ensures proportional risk management, and avoids unnecessary market distortion. Strengthening ENISA's coordinating role, ensuring meaningful stakeholder engagement, and promoting harmonised implementation under NIS2 will be essential to delivering both security and simplicity. A framework grounded in technical evidence, operational feasibility, and market realities will better support innovation, investment, and long-term resilience across Europe's digital infrastructure.

EuroISPA
Rue de la Loi 38, 1000 Brussels
secretariat@euroispa.org
EU Transparency Register: 54437813115-56