EuroISPA
The world's largest association of Internet Service Providers

EuroISPA Contribution to the CSA Review

June 2025

1. Maintain a strictly technical scope for certification
2. Strengthen ENISA's mandate and coordination role
3. Enable simplification and harmonisation across frameworks
4. Ensure proportionate compliance pathways for SMEs
5. Exempt internally developed tools not placed on the market
6. Recognise the importance of open-source and small-scale developers

EuroISPA welcomes the opportunity to contribute to the European Commission's review of the Cybersecurity Act (CSA). As the voice of European Internet Services Providers, EuroISPA supports a **targeted revision of the Regulation (Option 3)**, with a clear focus on strengthening ENISA's mandate in a technical capacity, enhancing harmonisation across Member States and legislative frameworks, and simplifying compliance obligations – especially for small and medium-sized companies (SMEs). To that end, EuroISPA highlights the following key considerations:

1. Maintain a strictly technical scope for certification

Certification schemes developed under the CSA should remain exclusively technical in nature. EuroISPA strongly believes that non-technical considerations – such as national or sovereignty-based requirements – should not be part of cybersecurity certification schemes. Introducing such criteria undermines the technical legitimacy and neutrality of the schemes, creates fragmentation across Member States, and risks harming the competitiveness and security of European businesses. Furthermore, localisation requirements, notably for cloud services (e.g. like in the EUCS) would be detrimental to cybersecurity in a technical sense. Therefore, certification should be based on widely recognised international standards and technical benchmarks that ensure both interoperability and robust cybersecurity across borders. Preserving the technical scope is essential to uphold the CSA's credibility and facilitate widespread adoption.

2. Strengthen ENISA's mandate and coordination role

EuroISPA believes that ENISA's mandate should be reinforced to support consistency and coherence in the implementation of cybersecurity requirements across the EU. The agency should play a central role in identifying areas of regulatory divergence between Member States and proposing measures to address them. It should also provide clear guidance on the applicable standards for compliance, particularly by promoting the use of international standards like ISO/IEC 27001. Furthermore, ENISA should be empowered to participate meaningfully in international standardisation bodies to ensure that EU interests are reflected in global frameworks. Transparency and inclusiveness in the development of certification schemes should also be improved – stakeholders must have timely access to drafts and a meaningful say throughout the process to improve both trust and outcomes.

3. Enable simplification and harmonisation across frameworks

Simplification of obligations across EU legal instruments is essential. Currently, companies face multiple and potentially overlapping cybersecurity-related reporting obligations under NIS2, the Cyber Resilience Act (CRA), the GDPR, and the Digital Operational Resilience Act (DORA). EuroISPA calls for harmonised reporting thresholds across these frameworks, along with the establishment of a single reporting point for cybersecurity incidents in each Member State. In addition, harmonisation should apply not only geographically across the EU but also across sectors and legislative instruments. Streamlined obligations covering scope, reporting, security measures, standards, and oversight will significantly reduce compliance burdens while improving effectiveness.

4. Ensure proportionate compliance pathways for SMEs

To support the wide diversity of actors in the digital ecosystem, including SMEs, the revised CSA should introduce proportionate compliance pathways. Specifically, SMEs as defined in Recommendation 2003/361/EC should be able to follow simplified procedures, including the option to self-assess and self-declare compliance using templates provided by ENISA. These measures will help ensure that the CSA does not unintentionally overburden smaller players, which often operate with limited resources but are critical to the EU's digital economy.

5. Exempt internally developed tools not placed on the market

EuroISPA recommends the introduction of a clear and general exemption for software, firmware, and ICT components that are developed in-house by companies for the sole purpose of delivering their own services. Certification should only be required when such tools are placed on the market, redistributed externally, or used in national critical infrastructure contexts. This approach avoids unnecessary regulatory burdens on internal tools that are not intended for broader commercial or public use.

6. Recognise the importance of open-source and small-scale developers

The revised CSA should explicitly recognise the essential role of open-source communities and artisanal developers in Europe's cybersecurity ecosystem. These actors contribute significantly to digital resilience and innovation and should not be excluded or discouraged by certification schemes that are overly complex or costly. Their work strengthens Europe's technological diversity and sovereignty and should be actively supported through proportionate, inclusive regulatory design.

To conclude, EuroISPA calls for a balanced and future-proof revision of the Cybersecurity Act – one that reinforces its technical character, strengthens ENISA's coordinating role, simplifies compliance through harmonisation, and accommodates the wide range of actors that contribute to Europe's cybersecurity. EuroISPA remains committed to engaging constructively with the European Commission to shape a digital regulatory framework that enhances security without stifling innovation or imposing disproportionate burdens on key stakeholders.

Established in 1997, EuroISPA is the world's largest association of Internet Services Providers Associations, representing over 3,300 Internet Service Providers (ISPs) across the EU and EFTA countries. EuroISPA is recognised as the voice of the EU ISP industry, reflecting the views of ISPs of all sizes from across its member base.