20 June 2025

Feedback of

ACT | The App Association
(Transparency Reg. # 72029513877-54)
Rue Belliard 40,
1000 Brussels, Belgium

to the

European Commission

regarding its

EU Cybersecurity Act

Introduction and statement of interest

ACT | The App Association (hereafter 'App Association') welcomes the opportunity to submit comments to the European Commission's consultation on its revision of the Cybersecurity Act.

The App Association is a policy trade association for the small business technology developer community. Our members are entrepreneurs, innovators, and independent developers within the global app ecosystem that engage with verticals across every industry. We work with and for our members to promote a policy environment that rewards and inspires innovation while providing resources that help them raise capital, create jobs, and continue to build incredible technology. Today, the ecosystem the App Association represents—which we call the app economy—is valued at approximately €86 billion and is responsible for over 1.3 million jobs in the European Union (EU).[1]

ENISA mandate

The App Association welcomes ENISA's new mandate as the empowerment of such agency will lead to more clarity and stability. Currently the lack of harmony between Member States is creating legal uncertainties and therefore mandating ENISA to increase operational cooperation at the EU level, helping EU Member States who wish to request it to handle their cybersecurity incidents, and supporting the coordination of the EU in case of large-scale cross-border cyberattacks and crises, is something welcomed by the App Association,

We support ENISA's role in setting up and maintaining the European cybersecurity certification framework by preparing the technical ground for specific certification schemes. Small and medium-sized entities (SMEs), such as our members, have strong incentives to implement stringent cybersecurity measures and increase their resilience due to both market dynamics and because it is the responsible thing to do. A cyberattack for a small business can mean loss of reputation and constitute an existential threat.

Certification schemes are important to our members, who place a strong emphasis on cybersecurity. We appreciate the value of certification marks in enhancing consumer trust, which helps facilitate market access. But for this framework to be truly effective and inclusive, it must:

- Be designed with the needs and capacities of SMEs in mind.
- Include transparent guidance and clear technical standards to avoid regulatory ambiguity.
- Engage the SME developer community early and throughout implementation, ensuring that our perspectives and constraints are meaningfully reflected.

Alignment with international standards for cybersecurity risk management

Representing a community of SMEs dedicated to raising the EU's cybersecurity posture writ large, numerous App Association members invested in the success of the EUCC seek to ensure that their existing cybersecurity practices, most notably those based on international standards like ISO/IEC

[1] *See* https://actonline.org/wp-content/uploads/Deloitte-The-App-Economy-in-the-EU-2020.pdf.

27001,[2] align with the Act's goals and expectations. We note that both the Act and ISO/IEC 27001 emphasise the importance of systematic governance, risk management, and continuous improvement in cybersecurity. We also appreciate that the certification schemes established under the EU Cybersecurity Act seem to be designed to be compatible with widely recognised international standards, which we interpret to mean that if an organisation is already certified to ISO/IEC 27001, such an organisation is well position to comply with EU requirements. We request that the EC memorialise this alignment and confirm the alignment we describe above; and further clarify that certification to ISO/IEC 27001 provides a means, or at minimum a strong presumption of, compliance with EUCC certification requirements.

The current ECCF and the challenges related to ICT supply chain security

We appreciate the value of certification marks in enhancing consumer trust, which help facilitate market access. This is particularly crucial for SMEs that may not have the same brand recognition and consumer loyalty as larger enterprises. Across consumer and enterprise verticals, end user confidence through certification programs can provide SMEs with an opportunity to demonstrate their commitment to cybersecurity and EU standards, and therefore provide a competitive edge.

Moreover, we welcome the streamlined certification process offered by the EUCC, especially regarding the consistency it creates throughout EU Member States in the cybersecurity certification process. We recognise that this helps reduce administrative burdens and costs associated with following fragmented national certification systems.

However, we also have several concerns. We hope that the Commission will continue to consider the effects of the EUCC on SMEs, such as our members, both during and after the implementation of the Regulation. Although the EUCC is voluntary, it demonstrates a high level of protectionism of the availability, authenticity, integrity, and confidentiality of ICT products' data and functions. This may have a significant impact on growing industries like the internet of things (IoT) and disproportionately affect small businesses with limited resources.

Therefore, we urge the Commission to consider the additional negative impact further requirements could have in terms of costs and implementation efforts for SMEs, such as the certification schemes proposed by the Cyber Resilience Act, and to take concerted efforts to educate and support SMEs. Compliance with cybersecurity requirements is difficult to achieve and maintain and requires proactive monitoring and security management before and after a product is on the market.

More specifically, the App Association appreciates European Commission (EC) efforts to account for the limited resources SMEs typically have, and we support the use of self-certification for low-risk use cases. For medium- and high-risk use cases, however, we caution against creating high-cost barriers for SMEs that third-party certifications can create. Mandates for third-party certifications from Information Technology Security Evaluation Facilities, while intended to raise standards, can place a heavy burden on SMEs. The costs of certification (including fees, audits, and staff time) can strain limited budgets and divert resources from growth activities. SMEs often lack the specialised personnel to handle complex compliance requirements, making the process

[2] https://www.iso.org/standard/27001.

overwhelming and time-consuming. Required upgrades and new procedures can disrupt daily operations, while ongoing administrative tasks to maintain certification add further strain. Ultimately, these mandates can exclude SMEs from markets or contracts they can't afford to certify for, limiting their competitiveness and ability to grow. The App Association therefore requests continued focus by the EC on ensuring that SMEs are not disadvantaged by mandates for third-party certifications on medium- and high-risk ('important' and 'critical') use cases.

Further, fully leveraging technical measures, including end-to-end encryption, is a critical element to protecting data broadly, by enabling key segments of the economy, from banking to national security to healthcare, through protecting access to, and the integrity of, data. Encryption's role should not be understated; without encryption, entire economies and industries are put a significantly heightened risk of their data being compromised. The App Association strongly believes that the Commission should recognise the vital role encryption and other technical measures play in securing data.

Finally, the App Association urges the EC to ensure that it is mindful of regulatory overlap issues. Many SMEs operate in sectors affected by multiple EU laws, such as the NIS2 Directive and the Cyber Resilience Act. Harmonising requirements and providing clear cross-references would help SMEs avoid duplication of effort and reduce administrative burdens.

Simplification of cybersecurity measures and reporting obligations

Simplification is key for SMEs to innovate and grow. The current regulatory landscape has led to overregulation and administrative burdens making it difficult for SMEs to do business in Europe. Significant administrative burden is placed on companies for the purposes of reporting incidents, and particularly those offering their services across several EU Member States, sometimes needing to file multiple reports within 24-72 hours and often in different languages. This administrative burden is intensified in situations where companies are unable to rely on one-stop-shop mechanisms.

That is why establishing a centralised alert mechanism allowing companies to notify incidents to a single reporting platform would be beneficial for SMEs. We also recommend developing a single incident reporting mechanism template to enable providers to file a single notification to all authorities in order to streamline reporting obligations within feasible deadlines. It is key to streamline cybersecurity and technical documentation requirements between the General Data Protection Regulation, Cyber Resilience Act, Network and Information Security 2 Directive and the Cybersecurity Act in order to avoid duplications and minimise additional burdens.[3]

Centralised, easy-to-understand guidance would also make a significant difference for SMEs. A single EU portal offering practical advice, sector-specific checklists, and up-to-date information in all official languages would help SMEs find the resources they need without getting lost in legal jargon. This portal could also connect SMEs with national and local support services, training opportunities, and peer networks.

[3] DOT Report page 22.

Financial and technical support for SMEs is also crucial. The EU should expand grant programs and subsidies to help SMEs cover the costs of compliance. Providing access to free or affordable cybersecurity tools and automated risk assessment platforms would further reduce the barriers to entry.

The App Association remains available to provide further input and welcomes the opportunity to contribute to policies that address SMEs' challenges while fostering a competitive and innovative business environment.

Sincerely,

Mike Sax
Founder and Chairperson

Maria Goikoetxea
Policy Manager

Giulia Cereseto
Policy Associate