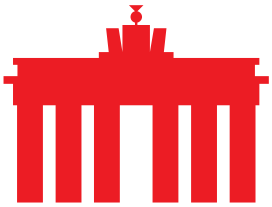

WE ARE SHAPING THE INTERNET.
YESTERDAY.TODAY.BEYOND TOMORROW.

POSITION PAPER

on the Call for Evidence for an Impact Assessment of the Revision of the Cyber Security Act (CSA)

Berlin, 20.06.2025

On 11 April 2025, the European Commission launched a consultation on the review of the Cybersecurity Act. This initiative is part of the Commission's current work programme, which places a strong focus on simplification alongside other points. The aim is to streamline existing cybersecurity regulations, strengthen resilience, promote EU-wide harmonisation and reduce bureaucracy.

The European Commission's 2025 work programme prioritizes simplification to enhance the EU's prosperity, competitiveness, and resilience. Following the Draghi report's findings on regulatory complexity hindering Europe's economic potential, the Commission is launching a major initiative to streamline EU legislation, making rules clearer, faster to implement, and easier to navigate. A key part of this agenda is the revision of the Cybersecurity Act (CSA) which established ENISA's permanent mandate and the European Cybersecurity Certification Framework (ECCF) for voluntary ICT certifications. The 2025 amendment will also allow certification schemes for managed security services.

The CSA revision aims to simplify and harmonize cybersecurity rules, including more agile and efficient reporting mechanisms to avoid duplication. It supports the broader simplification goal by reducing administrative burdens for companies and public authorities. It will also reassess ENISA's mandate in light of its expanded responsibilities under recent legislation such as NIS2, the Cyber Resilience Act, the Cyber Solidarity Act, and DORA. Additionally, the functioning of the ECCF will be evaluated, as three certification schemes are currently in progress. To ensure cybersecurity policy remains effective and innovation-friendly, the Commission focuses on ENISA's mandate, the ECCF's effectiveness, and simplification of cybersecurity and incident reporting obligations.

eco welcomes the Commission's initiative to streamline cyber security measures and strengthen cyber resilience while simplifying and improving EU policies and laws. eco would like the Commission to take the following points into account when revising the CSA:

1. ENISA's mandate

ENISA was initially given a broad mandate to meet the EU's cybersecurity needs. However, in the five years since the adoption of the Cybersecurity Act (CSA), the cybersecurity landscape has grown significantly more complex, with a notable rise

in the number of attacks. In response, new legislative measures have expanded ENISA's role to address these growing challenges and to strengthen support for EU cybersecurity stakeholders both within the EU and internationally, particularly in light of an increasingly unstable geopolitical environment.

Since the adoption of the 2019 Cybersecurity Act, ENISA has not only grown considerably in terms of personnel, but its remit has also expanded considerably due to additional cybersecurity regulation. Nevertheless, given the current geopolitical security challenges and the scale of global cyber threats, its financial resources remain limited compared to other EU bodies. As a result, ENISA continues to depend strongly on active engagement with stakeholders. While active stakeholder involvement is important and welcome, ENISA's strength lies in its independence and objectivity, which ideally underpin its key European role. The Agency's engagement strategy has increasingly focused on the involvement of EU institutions and experts. The political landscape and pushes for technological sovereignty has affected ENISA to operate freely. Therefore, it is important to boost ENISA's role as the independent expert on European Cybersecurity. In order to operate independently and attract necessary resources, staff, and experts to the benefit of its mandate, ENISA has to leverage its public standing among the global community.

ENISA's international strategy is welcome and should be followed by further initiatives to drive a clearer, sharper and more autonomous agenda and to engage its international public and private partners. The recommendation should be developed in close consultation with the national authorities responsible for cybersecurity in the EU.

To enable ENISA to keep pace with rapid and complex technological advancements, it is important that the agency maintains an organizational environment that supports flexibility. This includes aligning its internal structure, processes, and work program accordingly. Agility is key for ENISA to effectively adopt cutting-edge technologies in fulfilling its mission. Such adaptability would strengthen its role in shaping relevant policy and contributing to security discussions on emerging and evolving threats.

Although ENISA does not serve as a regulator or policymaker, it plays a crucial role in shaping key policy initiatives within the EU. This involvement has proven beneficial, as the Agency has developed strong policy expertise that enables it to contribute even more effectively to the policy-making process. By strengthening its public-private network and expanding its presence in Brussels and EU member state capitals, ENISA can gain deeper insight into national, regional, and EU-wide priorities and policy developments. This improved understanding would support more targeted resource allocation, ensuring that ENISA's activities align with current needs. A greater presence will also enable ENISA to foster stronger mutual understanding between EU institutions (such as the Commission, Council, and Parliament) and the stakeholders they represent. Therefore, ENISA should be granted greater autonomy in strengthening its expertise in cybersecurity policy.

This can be achieved through sustained investment and the establishment of structured relationships with regulators and policymakers in all 27 EU Member States, as well as with the European Parliament and the Council.

2. European Cybersecurity Certification Framework

The revision aims to examine key issues concerning the European Cybersecurity Certification Framework (ECCF), which plays a vital role in enhancing cybersecurity to safeguard industries, citizens, and critical infrastructure from both internal and external threats. However, the evaluation of the Cybersecurity Act (CSA) has identified areas for improvement, particularly in relation to the adoption and governance processes, the distribution of roles and responsibilities among Member States, the European Commission, and ENISA, as well as the formalization of the maintenance phase of certification schemes. A potential revision to the ECCF, with the aim of enhancing clarity, efficiency, and stakeholder involvement is being discussed.

Ensuring alignment with international standards and best practices is essential. Such harmonization not only lowers certification costs but also fosters cross-border and cross-technology innovation. Developing cybersecurity standards from the ground up is resource-intensive; by building on established, proven frameworks, governments can accelerate progress, enhance the overall cybersecurity posture, and facilitate international cooperation and knowledge sharing. Furthermore, aligning cybersecurity certification with existing global standards will strengthen the ability of European companies to compete and operate in international markets.

3. Simplification of cybersecurity and incident reporting obligations

The revision of the CSA also aims to collects stakeholders' input on the potential simplification of cybersecurity legislation in line with the European Commission’s simplification agenda. It focuses on gathering views on whether incident reporting requirements and cybersecurity risk management could be further streamlined, with a view to potentially reducing administrative burden.

EU regulation has increased significantly in recent years. In addition to the very welcome cyber regulation, many new laws have been introduced. This is not to be criticised in connection with cyber security. However, the abundance of requirements leads to massive reporting obligations. Reporting obligations, for which there are different deadlines and requirements and their exceptions, which unnecessarily fragment the internal market, are a heavy burden on companies in some cases. Targeted adjustments to simplify reporting obligations and faster reporting channels are therefore very welcome.

4. Conclusion

eco welcomes the initiative and appreciates the Commission's effort to revise the Cyber Security Act. Strengthening ENISA's independent role is essential to address today's complex cybersecurity challenges. Greater autonomy, sufficient resources, and deeper engagement across the EU will enable the Agency to better support policy development, foster international cooperation, and shape a forward-looking European cybersecurity agenda.

Revising the European Cybersecurity Certification Framework should focus on improving clarity, governance, and stakeholder involvement while aligning with international standards to boost efficiency, innovation, and global competitiveness.

Simplifying cybersecurity legislation and streamlining reporting obligations are essential to reduce administrative burdens and improve efficiency. Targeted adjustments can help prevent fragmentation of the internal market and ease compliance for companies without weakening cybersecurity.

About eco: With approximately 1,000 member companies, eco (international.eco.de) is the leading Association of the Internet Industry in Europe. Since 1995, eco has been highly instrumental in shaping the Internet, fostering new technologies, forming framework conditions, and representing the interests of its members in politics and international forums. eco has offices based in Cologne, Berlin and Brussels. In its work, eco primarily advocates for a high-performance, reliable and trustworthy ecosystem of digital infrastructures and services.