Cybersecurity Act 2

2026/0011(COD) - 20/01/2026 - Legislative proposal

PURPOSE: to strengthen the EU cybersecurity framework in response to evolving cyber threats, increased digitalisation, and heightened geopolitical risks affecting information and communication technologies (ICT) supply chains.

PROPOSED ACT: Regulation of the European Parliament and of the Council.

ROLE OF THE EUROPEAN PARLIAMENT: the European Parliament decides in accordance with the ordinary legislative procedure and on an equal footing with the Council.

BACKGROUND: since the adoption of Regulation (EU) 2019/881 of the European Parliament and of the Council (The Cybersecurity Act 2), the geopolitical, technological and policy landscapes have undergone significant transformations. Cyberattacks have surged and became more sophisticated, targeting critical infrastructure, businesses, and the general public, with the ransomware activity at its core. Emerging technologies like the artificial intelligence (AI) and quantum computing are reshaping the tools of defence and the tactics of adversaries.

This proposal is part of a package of measures that aims at aligning the Union’s cybersecurity framework with the needs of stakeholders in an increasingly sophisticated cyber threat landscape and complex geopolitical reality.

The objective of the proposed Regulation should be considered as part of the overarching goals of the Cybersecurity Act revision package involving the proposal for a Regulation by the European Parliament and the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881.

CONTENT: the present proposal reviews Regulation (EU) 2019/881 which sets out the current mandate and tasks for ENISA and the European Cybersecurity Certification Framework (ECCF). It is proposed that ENISA's revised mandate and amendments to the ECCF be established under the same legal instrument, using the instrument of a **regulation**. The proposal for the revision of the CSA has a clear focus on **streamlining, prioritising and codifying tasks across cyber-related legislations** could be achieved only at EU level and there isn't such initiative that currently exists. The new proposal further strengthens supply chain security and the cybersecurity sector within the EU and enhance the preparedness and resilience of the Member States and industry.

More specifically, the Regulation aims to:

Reinforce the mandate and role of ENISA as the EU Agency for Cybersecurity

Since the adoption of the first Cybersecurity Act in 2019, ENISA has grown as a cornerstone of the EU cybersecurity ecosystem. The revised Cybersecurity Act enables ENISA to help the EU and its Member States understand the common threats. It also enables them to prepare and respond to cyber incidents.

The proposal sets out ENISA’s tasks regarding operational cooperation in relation to Member States, Union entities and CERT-EU, the computer security incident response teams (CSIRTs) network, EU-CyCLONe and other stakeholders, including the issuance of guidelines and implementation of secure communications tools. ENISA will also help improve situational awareness of cyber threats and incidents by (among others) developing one or

more repositories of cyber threat intelligence, performing analysis and issuing **early alerts**.

In addition to these tasks, ENISA should provide tools and platforms, in particular the **single reporting platform**. The Agency must develop a common Union **vulnerability management service** capacity and provide vulnerability management services.

ENISA will continue to play a key role in further building a skilled cybersecurity workforce in Europe. It will do so by piloting the **Cybersecurity Skills Academy** and establishing EU-wide cybersecurity skills attestation schemes.

Strengthen and expand the European cybersecurity certification framework

The revised Cybersecurity Act will ensure that products and services reaching EU consumers are tested for security in a more efficient way. This will be done through a renewed European Cybersecurity Certification Framework (ECCF). The ECCF will bring more clarity and simpler procedures, allowing certification schemes to be developed within **12 months** by default. It will also introduce more agile and transparent governance to better involve stakeholders through public information and consultation.

Certification schemes, managed by ENISA, will become a **practical, voluntary tool** for businesses. They will allow businesses to demonstrate compliance with EU legislation, reducing the burden and costs. The renewed ECCF will be a competitive asset for EU businesses. For EU citizens, businesses and public authorities, it will ensure a high level of security and trust in complex ICT supply chains.

Address cybersecurity risks linked to ICT supply chains

The new Cybersecurity Act aims to reduce risks in the EU's ICT supply chain from third-country suppliers with cybersecurity concerns. It sets out a trusted ICT supply chain security framework based on a harmonised, proportionate and risk-based approach. This will enable the EU and Member States to jointly identify and mitigate risks across the EU's 18 critical sectors, considering also economic impacts and market supply.

The Cybersecurity Act will enable the mandatory derisking of European mobile telecommunications networks from high-risk third-country suppliers, building on the work already carried out under the 5G security toolbox.

Enhance coherence, effectiveness and resilience of the EU cybersecurity framework

The proposal sets out provisions relating to rules on the issuance of European cybersecurity certificates including those at the assurance level ‘high’. Furthermore, it lays down rules for harmonising European cybersecurity certification schemes with national cybersecurity certification schemes and cybersecurity certificates and provides for the possibility of international recognition of European cybersecurity certificates, based on the equivalence principle. Rules are laid down for a **peer review** mechanism between authorities, ensuring equivalent standards across the Union, and for cooperation between those authorities in the ECCG.

Budgetary implications

The estimated budget of ENISA was estimated at EUR 341 million for 7 years or yearly average budget of EUR 49 million (projection for 2028 to 2034). This represents **81.5% increase** to the budget of the Agency in 2025. The generated benefits of the proposed initiative will be significant with up to EUR 14.6 billion of cost savings for businesses. **Fee mechanisms** have been introduced to contribute to the ENISA’s budget, namely, fees from issuing authorisations for skills attestations, fees from testing tools service and fees from supporting the maintenance of the European Cybersecurity Certification schemes. The expected

generated benefit for the EU budget is estimated at approximately, EUR 18.5 million over 7-year period from 2028 to 2034.