# Commission Proposes Reform of the Cybersecurity Act

**Anna Pingen**

eucrim
European Law Forum: Prevention • Investigation • Prosecution

**News**

**AUTHOR**

**Anna Pingen**
Researcher
Max Planck Institute for the Study of Crime, Security and Law

Preprint eucrim 2025, Vol. 20(4)
ISSN: 1862-6947
https://eucrim.eu

On 20 January 2026, the European Commission presented a new cybersecurity package aimed at strengthening the European Union's resilience against cyber threats. The initiative included a proposal for a revised Cybersecurity Act that would repeal and replace Regulation (EU) 2019/881 and significantly expand the EU's cybersecurity governance framework.

According to the Commission, the reform responds to the rapidly evolving cyber threat landscape, marked by increasingly sophisticated attacks on critical infrastructure, businesses, and public institutions. The proposal seeks to strengthen the EU's capacity to prevent, detect, and respond to cybersecurity incidents while reducing fragmentation across the digital single market.

**Reform of the Cybersecurity Act**

The proposed regulation – referred to as the "Cybersecurity Act 2" – would substantially revise the mandate of the EU Agency for Cybersecurity (ENISA). ENISA would take on expanded operational and coordination tasks, including the issuance of early alerts on cyber threats, support for responses to ransomware attacks (together with Europol and the EU CSIRTs network), and the development of vulnerability management services across the EU.

The agency would also be tasked with strengthening operational cooperation between Member States and supporting the implementation of EU cybersecurity legislation, such as the NIS2 Directive and the Cyber Resilience Act. In addition, ENISA would play a larger role in cybersecurity exercises, incident response coordination, and capacity-building initiatives aimed at strengthening the cybersecurity workforce in the EU.

**Reform of the European cybersecurity certification framework**

Another central element of the reform concerned the European Cybersecurity Certification Framework (ECCF), originally introduced in 2019 but criticised for slow implementation. The proposal aimed to simplify and accelerate the adoption of certification schemes by introducing clearer procedures and a maintenance mechanism for existing schemes.

Under the revised framework, ENISA would prepare certification schemes, which the Commission could adopt following consultation with Member States and stakeholders. Certification would remain voluntary but could serve as proof of compliance with various EU cybersecurity obligations. The framework would also expand its scope to include not only ICT products and services but also the cybersecurity posture of organisations.

The Commission argued that the updated framework would make certification a practical compliance tool for companies operating under multiple EU cybersecurity regimes while reducing regulatory fragmentation.

**New EU framework for ICT supply chain security**

The reform package also introduces a new trusted ICT supply chain security framework aimed at addressing non-technical cybersecurity risks linked to suppliers. The Commission proposed a harmonised EU mechanism for identifying critical ICT assets and assessing supply chain risks, particularly where suppliers are linked to third countries posing cybersecurity concerns.

The framework would allow the Commission, following coordinated risk assessments, to designate high-risk suppliers and impose mitigation measures or restrictions on their involvement in critical ICT infrastructure. These measures could include limitations on the use of certain equipment in essential sectors or requirements to phase out high-risk components within defined transition periods.

The proposal builds on earlier initiatives such as the 5G security toolbox, extending risk-management approaches to ICT supply chains more broadly.

**Simplifying compliance with EU cybersecurity rules**

In parallel with the revised regulation, the Commission also pro-
posed targeted amendments to the NIS2 Directive to simplify compliance obligations. The changes are in-
ten-
ded to clari-
fy jurisdiction-
al rules, streamline ransomware reporting, and reduce regulatory burdens for companies operating across multiple Membe

Accord-
ing to the Commis-
sion, the simplifica-
tion meas-
ures could reduce compliance costs for thousands of companies while improving coordination between national authoritie

**Next steps**

The legislative package will now be negotiated between the European Parliament and the Council.

---