European Commission - Press release

Commission strengthens EU cybersecurity resilience and capabilities

Strasbourg, 20 January 2026

Europe faces daily cyber and hybrid attacks on essential services and democratic institutions, carried out by sophisticated state and criminal groups. The European Commission has today proposed a **new cybersecurity package** to further strengthen the EU's cybersecurity resilience and capabilities in the face of these growing threats.

The package includes a proposal for a **revised Cybersecurity Act**, which enhances the security of the EU's Information and Communication Technologies (ICT) supply chains. It ensures that products reaching EU citizens are cyber-secure by design through a simpler certification process. It also facilitates compliance with existing EU cybersecurity rules and reinforces the EU Agency for Cybersecurity (ENISA) in supporting Member States and the EU in managing cybersecurity threats.

Bolstering the security of ICT supply chains in the EU

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.

Recent cybersecurity incidents have highlighted the major risks posed by vulnerabilities in the ICT supply chains, which are essential to the functioning of critical services and infrastructure. In today's geopolitical landscape, supply chain security is no longer just about technical product or service security, but also about risks related to a supplier, particularly dependencies and foreign interference.

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.

Simplifying and enhancing 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. Beyond ICT products, services, processes and managed security services, companies and organisations will be able to certify their cyber posture to meet market needs. Ultimately, 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.

Facilitating compliance with cybersecurity rules

The package introduces measures to simplify compliance with EU cybersecurity rules and risk-management requirements for companies operating in the EU, complementing the single-entry point for incident reporting proposed in the Digital Omnibus. Targeted amendments to the NIS2 Directive aim to increase legal clarity. They will ease compliance for 28,700 companies, including 6,200 micro and small-sized enterprises. They will also introduce a new category of small mid-cap enterprises to lower compliance costs for 22,500 companies. The amendments will simplify jurisdictional rules,

streamline the collection of data on ransomware attacks and facilitate the supervision of cross-border entities with ENISA's reenforced coordinating role.

Empowering ENISA to boost Europe's cybersecurity resilience

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 presented today 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 agency will further support companies and stakeholders operating in the EU by issuing early alerts of cyber threats and incidents. In cooperation with Europol and Computer Security Incident Response Teams, it will support companies in responding to and recovering from ransomware attacks. ENISA will also develop a Union approach to provide better vulnerabilities management services to stakeholders. It will operate the single-entry point for incident reporting proposed in the Digital Omnibus.

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.

Next steps

The Cybersecurity Act will be applicable immediately after approval by the European Parliament and the Council of the EU. The accompanying NIS2 Directive amendments will also be presented for approval. Once adopted, Member States will have one year to implement the Directive into national law and communicate the relevant texts to the Commission.

For more information

Questions & Answers

Factsheet

Revised Cybersecurity Act

NIS2 targeted amendments

IP/26/105

Quote(s):

"Cybersecurity threats are not just technical challenges. They are strategic risks to our democracy, economy, and way of life. With the new Cybersecurity Package, we will have the means in place to better protect our critical ICT supply chains but also to combat cyber attacks decisively. This is an important step in securing our European technological sovereignty and ensuring a greater safety for all."
Henna Virkkunen, Executive Vice-President for Tech Sovereignty, Security and Democracy - 20/01/2026

Press contacts:

Thomas REGNIER (+32 2 29 91099)
Nika BLAZEVIC (+32 2 29 92717)

General public inquiries: Europe Direct by phone 00 800 67 89 10 11 or by email

Related media

College read-out / press conference by Henna Virkkunen, Executive Vice-President of the European Commission, on the Cybersecurity Act