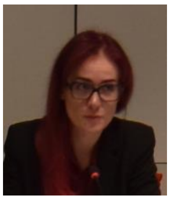
European Economic
and Social Committee

Single Market, Production and Consumption Section

3 March 2026: Cybersecurity Act - Expert hearing

On 3 March 2026, the INT Section meeting hosted an expert hearing on a Proposal for a revised Cybersecurity Act and targeted amendments to the NIS2 Directive as part of the new Cybersecurity Package published by the European Commission the 20 January 2026. In light of increasing geopolitical tensions, the European Commission recognizes the need to strengthen the EU's cybersecurity rules.



Marketá Gregorová, Rapporteur (Czechia – Piráti)

- Cybersecurity is a cornerstone of Europe's economic security and a key factor in maintaining trust in democratic institutions.
- Effective cybersecurity frameworks protect citizens not only from external threats but also from potential corporate misconduct.
- The security of the ICT supply chain remains vulnerable; the EU should decisively exclude high-risk suppliers from its critical digital infrastructure.
- Any assessment of suppliers should rely on strict, objective criteria and require a clear commitment to fundamental rights and human rights standards.
- Strengthening resilience enables EU companies to scale up and compete globally.
- Open-source solutions enhance transparency and accountability and require increased investment.
- New regulatory frameworks should ensure interoperability and portability of systems — for example, hospitals must be able to switch providers if systems fail or no longer meet requirements.
- Protecting end users must remain a central objective of EU cybersecurity policy.
- The revision of the Cybersecurity Act can serve as a blueprint for further strengthening and deepening the EU Single Market.

Zdenek Hrib, Rapporteur of the European Committee of the Regions and Member of the Local Assembly of the City of Prague

- Local and regional authorities will play a key role in implementing new cybersecurity rules, as they provide many frontline public services to citizens.
- Cities operate essential services—such as public transportation systems and e-government platforms—that must be protected against cyber threats.
- Smaller towns are equally important in the cybersecurity landscape, particularly because critical local infrastructure such as hospitals and healthcare services are frequent targets of cyberattacks.
- Levels of preparedness differ significantly across EU Member States and across local authorities, highlighting the need for tailored support and capacity-building.
- Cybersecurity is closely linked to citizens' trust in public institutions, making effective protection of public services a democratic as well as a technical priority.

- The Committee of the Regions opinion to be voted on in September identifies several priorities, including: avoiding overlaps between the revision of the Cybersecurity Act and the NIS framework; ensuring that EU cybersecurity certification schemes are relevant and accessible for local and regional authorities; promoting EU-level investigations into major cyber incidents; and coupling new regulatory requirements with administrative and technical support, particularly for smaller authorities.
- The Committee of the Regions strongly supports efforts to strengthen cybersecurity, but success will depend on practical implementation that takes into account the realities and specific needs of local and regional authorities.

Christina Rupp, Lead International Cybersecurity Policy

- Recent EU legislation – including the NIS2 Directive, the Cyber Resilience Act and the Cyber Solidarity Act – has significantly expanded ENISA's responsibilities, while also exposing structural challenges. The reform of ENISA should therefore prioritize consolidation over proliferation and ensure that the Agency is fully able to absorb and deliver on the many tasks it has been assigned in the last years.
- The proposal introduces new operational ambitions for the agency not yet covered in existing EU legislation (e.g. early alert service and a ransomware helpdesk for NIS 2 entities, ENISA membership in CSIRTs Network), raising concerns about overload and the unresolved question of whether ENISA should become an operational actor in its own right or remain primarily a support body for Member-state led operational actions.
- Amid an already crowded landscape of cybersecurity skills related certification initiatives, it is unclear why the Cybersecurity Skills Academy – particularly the development and maintenance of an individual cybersecurity skills attestation scheme – is given equal strategic weight to ENISA's other envisioned core pillars (policy implementation, operational cooperation, and certification).
- While strengthening the downstream impact of EU-level cybersecurity efforts is welcome, requiring each Member State to deploy at least two liaison officers to ENISA will be difficult given resource constraints. A network of ENISA-employed regional liaison officers covering three to five EU Member States could offer a more feasible alternative.
- The proposal rightly recognizes the need for increased financial and human resources. Any expansion of ENISA's mandate will need to be matched by adequate resources, which should be clearly reflected in the next Multiannual Financial Framework.

Rob Spiger, Director for Cybersecurity Policy, Microsoft

- Microsoft welcomes the revision of the Cybersecurity Act and the development of EU cybersecurity certification schemes, seeing them as important tools to strengthen trust in the digital ecosystem.
- ENISA should be further strengthened, including through increased funding and a stronger mandate for international cooperation.
- ENISA early alerts should be limited to publicly known vulnerabilities and complement the vulnerability reporting and coordinated disclosure practices under the Cybersecurity Resilience Act (CRA).
- Position ENISA technical specifications development as complementary to, not a substitute for, standardisation.

- The section on cryptography requires greater clarity, particularly regarding whether external organisations will be able to evaluate algorithms. If ENISA were to carry out these evaluations independently, this also raises questions about the availability of sufficient specialised expertise.
- Non-technical requirements should be clearly separated form certification schemes to improve clarity and implementation.
- The proposed timeline of 12 months to develop a cybersecurity certification scheme may be too short, and stakeholders would benefit from a clear roadmap to prepare for compliance.
- The certification scheme development process could be strengthened through a formal public consultation period, ensuring input from relevant stakeholders.
- Technical elements of certification schemes should be publicly available. However, for example, operational techniques used by service providers could remain confidential, rather than being made publicly available.
- Clarify and clearly delineate the use of extension profiles.
- The scope of certification should focus on specific business activities or services, rather than applying at the level of entire companies.
- Microsoft is supportive of addressing non-technical criteria in the trusted ICT supply chain framework proposed under CSA 2.0 for highly critical and critical sectors separately from technical criteria addressed through the certification framework.

Valentin Weber, Senior Associate Fellow - Center for Geopolitics, Geoeconomics, and Technology, German Council of Foreign Relations (DGCAP)

- Binding measures are needed to ensure harmonised implementation across the EU, in order to avoid the type of fragmentation that previously emerged in areas such as 5G policy.
- One shortcoming of the proposal concerns the timeliness of designating key ICT assets, which could delay effective risk management.
- The market impact must also be carefully considered, as prolonged processes and regulatory uncertainty can increase costs for businesses and public authorities.
- A comprehensive and continuous review of hypercritical components is necessary, including technologies such as solar converters and connected vehicles.
- The proposal currently lacks sufficient risk-mitigation measures to address data transfers to third countries, particularly where cybersecurity concerns may arise.
- The rules should clearly recognise that certain technological risks cannot be fully mitigated when dealing with companies located in countries that pose systemic cybersecurity risks.
- Intelligence-based assessments should therefore play a role in identifying high-risk countries, helping to inform risk evaluations and regulatory decisions.