Council of the European Union

Brussels, 6 May 2026
(OR. en)

8980/26

Interinstitutional Files:
2026/0011 (COD)
2026/0012 (COD)

CYBER 209
JAI 538
DATAPROTECT 146
TELECOM 214
MI 435
IND 318
CADREFIN 200
FIN 643
BUDGET 14
CSC 290
CODEC 845

COVER NOTE

From:	General Secretariat of the Council
date of receipt:	6 May 2026
To:	Delegations
Subject:	Proposal for a Regulation of the European Parliament and of 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 (The Cybersecurity Act 2) Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2022/2555 as regards simplification measures and alignment with the [Proposal for the Cybersecurity Act 2] - Opinion of the European Economic and Social Committee

Delegations will find attached the opinion on the above-mentioned proposals adopted by the European Economic and Social Committee on 29 April 2026. Other language versions, if needed, will soon be available on the following website: https://dmsearch.eesc.europa.eu/search/opinion

European Economic and Social Committee

OPINION

European Economic and Social Committee

Cybersecurity Act

---

a) Proposal for a Regulation of the European Parliament and of 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 (The Cybersecurity Act 2)
(COM(2026) 11 final – 2026/11 (COD)

and

b) Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2022/2555 as regards simplification measures and alignment with the [Proposal for the Cybersecurity Act 2]
(COM(2026) 13 final – 2026/12 (COD))

INT/1109

Rapporteur: **Miroslav HAJNOŠ**

www.eesc.europa.eu

EN

@EU_EESC @EuropeanEconomicAndSocialCommittee @european-economic-social-committee @eu_civilsociety @EESC

Advisor	Pavlina PAVLOVA (for the rapporteur)
Legislative procedures	EU Law Tracker EU Law Tracker
Referrals	a) European Parliament, 5/2/2026 Council of the European Union, 23/3/2026 b) European Parliament, 6/2/2026 Council of the European Union, 23/3/2026
Legal basis	Article 114 of the Treaty on the Functioning of the European Union
European Commission documents	COM(2026) 11 final – 2026/11 (COD) COM(2026) 13 final – 2026/12 (COD) Summary
Relevant Sustainable Development Goals (SDGs)	SDG 8 Decent work and economic growth SDG 9 Industry, innovation and infrastructure SDG 12 Responsible consumption and production SDG 17 Partnerships for the goals
Section responsible	Section for the Single Market, Production and Consumption
Adopted in section	15/4/2026
Adopted at plenary session	29/4/2026
Plenary session No	605
Outcome of vote (for/against/abstentions)	193/0/0

1. RECOMMENDATIONS

The European Economic and Social Committee (EESC)

1.1 **welcomes** the Commission's initiative to revise the Cybersecurity Act (CSA) and introduce amendments to the NIS 2 Directive, and **supports** the objectives of the package to strengthen the EU's resilience to cyber threats, improve legal clarity and institutional coordination, simplify compliance frameworks and reduce the administrative burden on regulated entities, while preserving the competitiveness and innovation capacity of the European market; **stresses** that cybersecurity and ICT supply chain security must be treated as matters of economic security and geopolitical resilience, not solely as technical or regulatory challenges;

1.2 **highlights** that the European Union Agency for Cybersecurity's (ENISA) mandate significantly contributes to enhancing the Union's cyber resilience. The proposed clarification of ENISA's role should first and foremost address the consolidation of the Agency's mandate and the absorption of the new tasks stemming from the requirements under the Union's expanded regulatory framework;

1.3 **cautions** that where the proposal expands the Agency's responsibilities, corresponding increases in resources and specialised staff must be ensured to support effective implementation. Any additional tasks assigned to ENISA should be explicitly conditional on the establishment of a mandatory workforce plan;

1.4 **highlights** that cybersecurity resilience depends on workforce skills, training and organisational culture. The proposed role for ENISA regarding the European cybersecurity skills framework and authorisations for skills attestations, which is transferable across Member States, is a welcome step, provided that the tasks of the relevant institutions and authorities are clearly defined, mutually reinforcing and do not duplicate existing certification;

1.5 **highlights** that cybersecurity is also a fundamental component of democratic resilience, stressing the growing risk of cyber threats targeting democratic processes, including elections, through disinformation campaigns, manipulation of digital infrastructure and foreign interference, and **calls for** strengthened EU-level coordination to protect electoral systems, including risk monitoring, information-sharing and support for Member States' election security frameworks;

1.6 **supports** the development, implementation and uptake of the certification schemes as a means of strengthening trust across the single market, while underlining its long-standing commitment to a harmonised Union cybersecurity framework based on legal certainty, transparency and proportionality, and to prioritising coherence and usability over regulatory accumulation;

1.7 **underlines** that certification must function as a genuine compliance enabler, in particular for cross-border and multi-country operators subject to overlapping cybersecurity obligations. The revised certification framework must include robust provisions on scheme maintenance, transparency, governance clarity and consumer protection;

1.8 **acknowledges** the proposal to establish a structured EU-level framework for the identification of key ICT assets and the development of proportionate risk mitigation measures, including, where justified, measures addressing high-risk suppliers, in line with de-risking ICT supply chains to reduce dependencies on suppliers established in, or controlled by, countries posing cybersecurity concerns; **stresses** that any measures concerning ICT supply-chain security must be based on clear, predictable and transparent requirements;

1.9 **calls** for full consideration of the economic impact and the downstream impacts of the proposed supply-chain intervention, including feasibility, availability of alternatives, lifecycle constraints, operational disruption risk, operational costs, effects on prices and service quality for end-users, labour-market impacts and innovation;

1.10 **underlines** the need to ensure that obligations under the revised framework are applied in a proportionate manner and do not result in the indirect or undue transfer of compliance burdens to actors outside its scope, avoid 'compliance dumping' and remain consistent with the objectives of simplification, legal clarity and SME-sensitivity underpinning the simplification agenda in the CRA and NIS 2 Directive;

1.11 **calls for** a systematic involvement of the social partners, SMEs, consumer organisations, relevant civil society organisations, academia and think tanks in the development, implementation and monitoring of schemes, to ensure that the framework is operationally fair, democratically intelligible and feasible in practice, and that it supports the Union's technological sovereignty and competitive advantage.

2. EXPLANATORY NOTES

Argument in support of recommendation 1.1

2.1 The CSA (Regulation (EU) 2019/881) is being revised in accordance with the requirement for a comprehensive evaluation of ENISA and the European cybersecurity certification framework (ECCF), addressing the increased complexity and diversity of cybersecurity-related policies, the stalled implementation of the ECCF and the growing ICT supply chain risks.

Arguments in support of recommendation 1.2

2.2 The revision expands and reorganises ENISA's tasks. The EESC considers that the priority of the proposal should be to consolidate and streamline ENISA's mandate and to absorb new tasks strictly in line with the CRA and the NIS 2 Directive.

2.3 **The EESC supports the establishment of a single-entry point for reporting incidents to streamline parallel reporting obligations under the NIS 2 Directive, DORA and sector-specific rules, with interoperable and standardised reporting templates, clearly defined reporting deadlines and content requirements. Such simplification must be operational and not merely formal: one comprehensive report should suffice for all relevant regulatory regimes.**

Arguments in support of recommendation 1.3

2.4 The proposed budget may not be sufficient to cover all tasks. Any expansion or reorganisation of tasks must be matched by adequate and sustainable financial resources and specialised staff to avoid creating an unfunded mandate, which could undermine ENISA's effectiveness and ability to demonstrate added value.[1] The EESC would further welcome supplementary resources and contribution agreements being incorporated into and reflected in the formal budget.

2.5 The proposal specifies that the Agency's budget would be partially covered by self-funding mechanisms through fees from supporting the maintenance of the European cybersecurity certification schemes, authorisation and skills attestation. This estimate is based on the expected uptake of certification across the Union and may not fully reflect actual uptake in practice.

2.6 **A mandatory workforce plan should address skills development, training needs and workload reallocation, accompanied by appropriate arrangements to prevent excessive overtime and burnout, and by minimum capacity safeguards ensuring that core deliverables can continue to be carried out effectively.** The planned appointment of two liaison officers per Member States may prove unrealistic, especially for smaller and under-resourced Member States.

Arguments in support of recommendation 1.4

2.7 The EESC reiterates that cybersecurity resilience depends on workforce skills, training and organisational capacity. The proposed skills attestation schemes can contribute to this objective, provided that they remain practical, proportionate and accessible.

2.8 Improving cybersecurity literacy among the general public is a necessary complement to professional skills development and should be fully encouraged across the EU. A population that is better informed about cyber risks, disinformation and safe digital behaviour contributes directly to reducing vulnerabilities at societal level. Such awareness is particularly important in an increasingly digitalised economy, where human factors remain a primary vector for cybersecurity incidents.

Arguments in support of recommendation 1.5

2.9 Cyber threats increasingly target democratic institutions and processes, including elections, through hybrid tactics such as disinformation, cyberattacks on electoral infrastructure and manipulation of public discourse. These risks have systemic implications for trust in public institutions and the functioning of democratic systems. The EESC therefore considers it essential to strengthen coordination at EU level and to support Member States in protecting electoral processes, while respecting national competences. Enhancing both institutional resilience and public awareness is a key component of safeguarding democracy in the digital age.

1 In its opinion on the CSA (OJ C 227, 28.6.2018, p. 86.), the EESC considered that ENISA's new permanent mandate would significantly contribute to enhancing the resilience of European systems. This direction was further acknowledged in the EESC's position on the CRA (OJ C 100, 16.3.2023, p. 101.), which states that it will be important for ENISA to be provided with the necessary resources to carry out the important and sensitive tasks entrusted to it effectively and in a timely manner.

Arguments in support of recommendation 1.6

2.10 The EESC supports certification schemes, including cyber posture certification for entities, as a means of simplifying compliance in practice, strengthening cybersecurity and building trust across the single market. The Committee supports alignment with the NIS 2 Directive through the targeted amendments proposed in the accompanying directive, with a view to reducing regulatory complexity, improving coherence across Union cybersecurity legislation, facilitating compliance for regulated entities and strengthening support for cross-border supervision.

Arguments in support of recommendation 1.7

2.11 Certification should reduce audits and compliance procedures. This requires proportional, risk-based schemes aligned with international standards (ISO/IEC) through meaningful mutual recognition and interoperable approaches, preserving global market openness and enabling EU-certified products and services to compete effectively.

2.12 Predictable timelines, clear procedures and proportionate costs are essential to ensure that SMEs and smaller service providers are not disadvantaged. A 'certify once, certify everywhere' approach must be the operational standard.

2.13 ENISA should ensure effective maintenance of European cybersecurity certification schemes and clarity of governance, addressing the lessons of the existing framework where limited uptake, lengthy procedures and insufficient operational clarity have undermined its effectiveness. To support trust and market uptake, ENISA shall make publicly accessible, clear and comparable information on the cybersecurity levels of certified products and services.

Arguments in support of recommendation 1.8

2.14 The proposal addresses the need to make the Union's economy and ICT supply chain more resilient in order to promote its own security and competitiveness. The EESC welcomes the Commission's initiative[2], in line with the view that the EU should not procure or integrate critical ICT components from countries that actively undermine European security interests.

2.15 Where risk mitigation measures lead to restrictions on or the phase-out of suppliers considered to present high cybersecurity risks, transition planning is essential. Transition plans should include asset inventories, dependency mapping, realistic replacement timelines and safeguards that ensure continuity of services. These conditions are necessary to ensure that the EU can strengthen supply chain security while avoiding operational disruption and cost shocks for operators and end-users.

Arguments in support recommendation 1.9

2.16 Assessments concerning economic impact must fully consider the practical application of the framework, especially where phasing-out or other restrictive measures are expected to be imposed on key providers and critical entities. ICT supply-chain controls can have significant operational

2 OJ C 227, 28.6.2018, p. 86.

and economic effects, and a systematic assessment of these impacts is necessary to support proportionality, legal certainty and social acceptance. The proposed measures risk limiting the freedom of contract for companies, and may have a substantial impact on telecom providers, cloud and data centres and any company that uses ICT technology and falls under the NIS 2 Directive. As a result, companies may face higher costs in terms of changing equipment and suppliers, which can be especially hard for SMEs and can reduce choice by excluding or restricting some vendors.

2.17 The EESC urges recognition that cybersecurity resilience depends on workforce development and safe working conditions for cyber professionals, including those in critical infrastructure sectors, where relevant to operational cybersecurity resilience.

2.18 The assessments of economic and social impacts should include relevant labour-market indicators. These should encompass, among other things, reskilling and upskilling requirements, training volumes and associated costs, workload implications for key functions such as IT, cybersecurity, procurement and compliance, as well as potential restructuring needs and transition measures aimed at preventing abrupt displacement effects.

Arguments in support of recommendation 1.10

2.19 Considering the proposal's potential to affect procurement choices, the process requires clear, objective and reviewable criteria, predictable procedures and a transparent rationale for any adopted measures. The rules affecting suppliers must be strictly risk- and evidence-based to protect service continuity and ensure investment predictability, otherwise they risk creating uncertainty, additional costs, disruption to the Union's market, and the shifting of obligations down the value chain, in particular to smaller suppliers and subcontractors. Entities should not face compliance obligations disproportionate to their size and capacity.

Argument in support of recommendation 1.11

2.20 Cybersecurity measures with significant implications for supply chains and public and private procurement must be developed and implemented through structured stakeholder involvement to assess economic and social impact in order to determine which risk-based measures are needed, appropriate, legally sound and operationally feasible. Consultation with social partners should constitute a structural element of such assessments rather than being treated merely as an optional good practice.

3. PROPOSED AMENDMENTS TO THE LEGISLATIVE PROPOSAL OF THE EUROPEAN COMMISSION

Amendment 1
linked to recommendation 1.4 and 1.5

Text proposed by the European Commission	EESC amendment
	Article 7 bis ***Cybersecurity awareness and democratic resilience*** ***1. ENISA shall support Member States and Union institutions in strengthening cybersecurity awareness and resilience of democratic processes, including elections, against cyber threats and hybrid interference.*** ***2. ENISA shall contribute to the development of Union-wide initiatives aimed at improving cybersecurity literacy among the general public, including awareness of disinformation, secure digital behaviour and risks related to democratic processes.***

Reason
Cyber threats increasingly target democratic institutions and electoral processes. Strengthening both institutional safeguards and public cyber literacy is essential to ensure democratic resilience and trust in the digital environment.

Amendment 2
linked to recommendation 1.8, 1.9, 1.10, 1.11

Text proposed by the European Commission	EESC amendment
	Article 103 bis ***Transition planning and proportional implementation*** ***1. Where mitigation measures under Article 103 include restrictions, phase-outs or replacement obligations, the Commission shall ensure such measures are accompanied by mandatory structured transition plans, additional to the transition periods provided for in Article 103(1).*** ***2. Transition plans shall include, at a minimum: (a) asset inventories and dependency mapping of affected ICT components; (b) realistic timelines for replacement or mitigation; (c) safeguards ensuring continuity of services in sectors of high criticality.*** ***3. Measures under this Title shall avoid undue operational disruption, shall not impose disproportionate costs relative to entity size and risk exposure, and shall prevent indirect transfer of compliance obligations to entities outside the scope of this Regulation.*** ***4. The Commission shall ensure systematic involvement of industry, SMEs, social partners and civil society in the preparation and evaluation of measures***.

Reason
This amendment requires structured transition plans and anti-cascading protections, ensuring supply chain measures are proportionate and do not transfer compliance burdens onto actors outside the Regulation's scope.

Brussels, 29 April 2026.

The President of the European Economic and Social Committee
Séamus BOLAND