Council of the European Union

Brussels, 22 May 2026
(OR. en)

9399/26

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

LIMITE

CYBER 229
JAI 606
DATAPROTECT 161
TELECOM 239
MI 489
IND 342
CADREFIN 220
FIN 697
BUDGET 19
CSC 316
CODEC 937

NOTE

From:	General Secretariat of the Council
To:	Permanent Representatives Committee/Council
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 Europan Parliament and of the Council amending Directive (EU) 2022/2555 as regards simplification measures and alignment with the [Proposal for the Cybersecurity Act] - Progress report

The Presidency has drawn up a progress report on the 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 the ICT supply chain security and repealing Regulation (EU) 2019/991 (The Cybersecurity Act 2), in order to report on the work carried out so far by the Council preparatory bodies and on the state of play in the examination of the proposal.

INTRODUCTION

1. On 20 January 2026, the Commission proposed a new cybersecurity package to strengthen the EU's cybersecurity resilience and capabilities. The package consists of a **Regulation** on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and Information and Communication Technologies (ICT) supply chain security and repeals Regulation (EU) 2019/881 (Cybersecurity Act). This Regulation ("Cybersecurity Act 2") is complemented by a **Directive** amending Directive (EU) 2022/2555 (NIS 2 Directive) as regards simplification measures and alignment with the [Proposal for the Cybersecurity Act].

2. Prior to the proposal, the Council, in its Conclusions on ENISA of 6 December 2024[1], invited the Commission to examine and further strengthen ENISA's role in supporting operational cooperation at the EU level and among Member States in enhancing cyber resilience, taking into account Member States' competences in this field. The Commission was also called on to ensure that ENISA's mandate to support Member States was focused and clearly-defined, with concrete strategic objectives and prioritised tasks, in addition to a more precise division of tasks and competences with respect to other actors. The Council also urged the Commission to use the opportunity of the Cybersecurity Act evaluation to find ways to have a leaner, risk-based as well as more transparent and faster approach to the development of EU cybersecurity certification schemes. Furthermore, in its Conclusions[2] of 21 May 2024 on the future of cybersecurity, the Council stressed its commitment to ensuring secure ICT supply chains and highlighted the relevance of non-technical risk factors, including undue influence by third States on suppliers and providers. Finally, the Council Conclusions[3] of 17 October 2022 on ICT supply chain security underlined the need to strengthen the resilience and security of ICT supply chains, considering the impact of geopolitical tensions and dependencies on ICT products and services.

---

1 16527/24
2 10133/24
3 13664/22

3. The purpose of the proposal for a Regulation, which is based on Article 114 TFEU, is to strengthen the Union's cybersecurity framework. It reinforces the role and tasks of the European Union Agency for Cybersecurity (ENISA) to support Member States and Union entities in achieving a high level of cybersecurity, resilience and trust in the Union. It aims at making the European Cybersecurity Certification Framework (ECCF) more effective and efficient in order to enable a faster scheme development and implementation. The proposal also establishes a Union framework on trusted ICT supply chain security, addressing non-technical risk factors and dependencies affecting the security of critical ICT infrastructure and services. It is accompanied by targeted simplification measures related to the implementation of the NIS 2 Directive[4], aimed at simplifying compliance requirements, reducing unnecessary administrative burden and increasing legal clarity.

4. The 'One Europe, One Market' roadmap[5] signed on the sidelines of the informal meeting of Heads of State or Government that was held in Cyprus on 24 April 2026, includes this proposal as one of the priority deliverables.

5. The European Parliament appointed Ms Gregorová Markéta (Greens/EFA) as rapporteur of the ITRE Committee, which is the committee responsible for the subject matter.

6. On 29 April 2026 the European Economic and Social Committee issued an opinion on the proposal[6].

---

4 OJ L 333, 27.12.2022, pp. 80.
5 8473/26
6 8980/26

STATE OF PLAY WITHIN THE COUNCIL PREPARATORY BODIES

7. A general presentation of the cybersecurity package took place at a meeting of the Horizontal Working Party on Cyber Issues (HWPCI) on 26 January 2026 and at a meeting of the Permanent Representatives Committee on 28 January 2026.

8. The HWPCI began to discuss the proposal on 2 February 2026 with a detailed presentation by the Commission. During this presentation the Commission also introduced the findings of the evaluation report, the financial statement and the impact assessment.

9. The HWPCI started the readthrough of the proposed Regulation on 23 February 2026.

10. Member States welcomed the proposal and generally supported its overall objectives, notably the strengthening of ENISA's support to Member States' operational cooperation and streamlining the certification framework. However, the discussions also showed that several aspects of the proposal would require further examination. Delegations requested further clarifications regarding the increased operational role and tasks envisaged for ENISA such as the issuance of early alerts, the creation of a ransomware helpdesk and ENISA's role in the CSIRTs network. Several delegations questioned the resource implications for Member States linked to the proposed contribution of two seconded national experts (SNEs) per Member State to support ENISA's tasks. The voting rules of the Management Board also require further discussions. The need for greater clarity and precision regarding definitions and concepts used throughout the proposal was stressed by delegations. The composition of the ENISA budget, notably the levying of fees also needed further clarifications.

11. The new provisions to make the certification process more effective and efficient were generally welcomed although a general need was identified for an increased participation of Member States throughout the certification process. The voluntary nature of certification was generally welcomed. However, delegations questioned some of the proposed deadlines under the certification framework.

12. The discussions on the Trusted ICT Supply Chain Framework highlighted several concerns among Member States. Delegations called for further clarifications on the methodology and procedures for the identification of key ICT assets and high-risk suppliers, as well as on the scope and possible impact of the proposed measures. The importance of ensuring an appropriate level of involvement of Member States was stressed by delegations.

13. Several delegations entered scrutiny reservations on different parts of the proposal, in particular regarding governance aspects, the use of implementing acts and the proposed mechanism for the identification of high-risk suppliers and ICT supply chain security.

14. Following the discussions in the HWPCI, Member States were invited to submit written comments on the provisions related to Title I on general provisions and Title II on ENISA. 23 Member States submitted contributions. Later, Member States were also invited to provide written comments on Title III on the European cybersecurity certification framework. 20 Member States took the opportunity to submit their position in writing.

15. On the basis of these written contributions from Member States and the work within the HWPCI, the Presidency will draw up a compromise text on Titles II (ENISA) and III (European Cybersecurity Certification Framework) which will be presented at the HWPCI meeting early June 2026.

16. Several Member States asked the Council Legal Service to examine the appropriateness of the legal basis.

17. The Presidency will start the readthrough on the simplification measures of the NIS 2 Directive at the end of May 2026.

18. Altogether, the HWPCI will have held a total of 15 meetings on the Cybersecurity Act 2 proposal under the Cyprus Presidency.

19. On the basis of the progress made under the Cyprus Presidency, the incoming Irish Presidency plans to continue work on this important file.

20. In the light of the above, the Permanent Representatives Committee and the Council are invited to take note of the progress made on the examination of the proposal for a Regulation.