Council of the European Union
General Secretariat

Interinstitutional files:
2026/0011 (COD)

Brussels, 18 May 2026

WK 6913/2026 INIT

LIMITE

CYBER	**IND**
JAI	**CADREFIN**
DATAPROTECT	**FIN**
TELECOM	**BUDGET**
MI	**CSC**
	CODEC

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From: To:	General Secretariat of the Council Horizontal Working Party on Cyber Issues
N° Cion doc.:	5611/26 + ADD 1 - 4
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): EU cybersecurity certification of cyber posture - Presentation by the Commission

Delegations will find in the annex a presentation on EU cybersecurity certification of cyber posture given by the Commission at the Horizontal Working Party on Cyber Issues meeting of 18 May 2026.

Revised Cybersecurity Act (CSA2) **Proposal**

EU cybersecurity certification of cyber posture

CNECT Presentation at the HWPCI – 18 May 2026

European Commission

Cyber posture (CP) scheme highlights I

CP certification allows the certification of **organisational cybersecurity of entities** with respect to at least one of the security objectives set out in Article 80(1)(q) – (w)

CP certification can **demonstrate compliance** and **presume conformity** where EU legal acts provide so (for now: only NIS2, see proposed Article 24(4) and (5) NIS2)

CP certification should in particular help entities providing **services across several MS** to demonstrate compliance [with NIS2]

Development of a CP scheme can benefit from the adoption of maximum harmonisation **implementing acts** under NIS2

Extension profiles allow demonstration of compliance with additional national security requirements (especially in the case of **minimum harmonization**)

CP scheme highlights II

Modular scheme based on relevant security objectives (Article 80(1)(q) – (w)) reflecting different approaches/specifics to cyber and data security in EU legal acts

No conformity self-assessment for presumption of conformity (Articles 78(2) and 82(8))

Continuous compliance with relevant security requirements model (Article 71(2)(c))

All conformity assessment activities **restricted to European Economic Area** (Article 82(8))

Involvement of the **NIS Cooperation Group** (Article 73(4) and 74(4))

Synergy and can supplement other **schemes** (e.g. EUCS, EUMSS)

Can be based on existing **frameworks, standards and specifications** (NIST, ISO/IEC, ETSI, CEN/TS)

Use cases of cyber posture certification

Modular avenue to demonstrate compliance

1. NIS2 Directive (see proposed NIS2 amendments - Article 24(4) and (5))
2. GDPR (no empowerment to activate presumption of compliance at the moment)
3. Sectoral cybersecurity legislation (e.g. NCCS in the energy sector)

NIS2 Directive – 3 use case examples

Maximum harmonized IAs under NIS2

- Reflecting technical and methodological requirements of the cybersecurity risk-management measures set out in NIS2 implementing acts

National extension profiles for transpositions

- An entity providing services across the EU can demonstrate compliance with all relevant extension profiles through a single certificate

Article 81(3)(c) of the CSA2 proposal

Minimum baseline for risk management measures

- Harmonisation of basic requirements
- Common denominator
- Suppliers for NIS2 entities and SMEs

Demonstration of compliance with NIS2

Possible procedure for demonstration of compliance with NIS2

Step 0 (optional): Adoption of Implementing Act under NIS2

Step 1: Development and adoption of a cyber posture certification scheme (“EUCP”)

Step 3 (where applicable): Development of extension profiles to cater for national transpositions

Step 4: Entities can obtain a certificate to demonstrate compliance with NIS2

Step 5: Entities are subject to the continuous testing, certification and inspection requirements as set out in the scheme*

Step 6: National competent authorities supervise and enforce compliance

* Where an entity obtained a certificate, the national competent authorities cannot subject the entity to regular and targeted security audits (Art 32(2)(b) and Art 33(2)(b) NIS2), see proposed Art 24(5) NIS2).

Thank you